2014 年 4 月 16 日
(改訂日:2014 年 5 月 2 日)
※改訂履歴は最終ページに記載

お客様各位

株式会社セゾン情報システムズ
HULFT 事業部

HULFT Series 製品における OpenSSL の脆弱性に対する報告

HULFT Series 製品における OpenSSL の脆弱性に対する報告をご案内いたします。

― 記 ―

1. 脆弱性の内容

遠隔の第三者が細工したパケットを送付することでシステムのメモリ内の情報を閲覧し、秘密鍵などの重要な情報を取得する可能性があります。

〈OpenSSL の脆弱性に関する注意喚起〉

http://www.jpcert.or.jp/at/2014/at140013.html

2. 調査結果

HULFT Series製品において、OpenSSLの上記脆弱性を内包しておりません。

〈HULFT Series製品 調査結果〉

製品名	調査結果
HULFT	➢ HULFT BB クライアント／HULFT BB サーバ・接続オプション OpenSSL のライブラリを使用しておりますが、脆弱性のある OpenSSL のバージョンは使用しておらず、脆弱性の原因となる機能も使用されません。 ➢ 上記以外 OpenSSL は使用しておりません。
HULFT-HUB	OpenSSL は使用しておりません。
HULFT-DataMagic	➢ UNIX/Linux 64 ビット版 Ver.2.2.0 OpenSSL のライブラリを使用しておりますが、脆弱性の原因となる機能は使用しておりません。 ➢ 上記以外 OpenSSL のライブラリを使用していますが、脆弱性のある OpenSSL のバージョンは使用しておらず、脆弱性の原因となる機能も使用されません。
HULFT クラウド	OpenSSL は使用しておりません。 Apache 等の Web サーバにつきましては、お客様にてご確認ください。
HDC-EDI Suite	OpenSSL は使用していません。
iDIVO	OpenSSL のライブラリを使用しておりますが、脆弱性のある OpenSSL のバージョンは使

	用しておらず、脆弱性の原因となる機能も使用されません。
SIGNAlert	➢ SIGNAlert Manager Web 監視オプション Ver.3.5.3 OpenSSL のライブラリを使用しておりますが、脆弱性の原因となる機能は使用しておりません。 ➢ 上記以外 OpenSSL のライブラリを使用しておりますが、脆弱性のある OpenSSL のバージョンは使用しておらず、脆弱性の原因となる機能も使用されません。

【改訂履歴】
2014/05/02　調査結果の詳細「<HULFT Series 製品　調査結果>」を追加しました。

以上