Intra-mart製品における

セキュリティ対策の現状

アジェンダ

- セキュリティ対策の現状
- IMARTタグのエスケープ機能

セキュリティ対策の現状について

- プロダクトデベロップメントグループ
- ホシ　リョウ ---------->

はじめに

- SaaS／Cloud環境でのintra-mart製品の利用の増加

- セキュリティはその性質上、継続的な強化が必要である。

  - 現在、intra-mart製品に関して脆弱性の再調査と対策を順次行っている。

※セキュリティに関してはファーストリリース時点で十分考慮している。

はじめに

- 継続対応している脆弱性
  - Cross Site Scripting　　(以降XSSとする)
  - SQL Injection
  - HTTP Response Splitting
  - システムの秘密情報の漏えい
  - ファイルアップロード機能の不備
  - Cross Site Request Forgeries (CSRFとする)

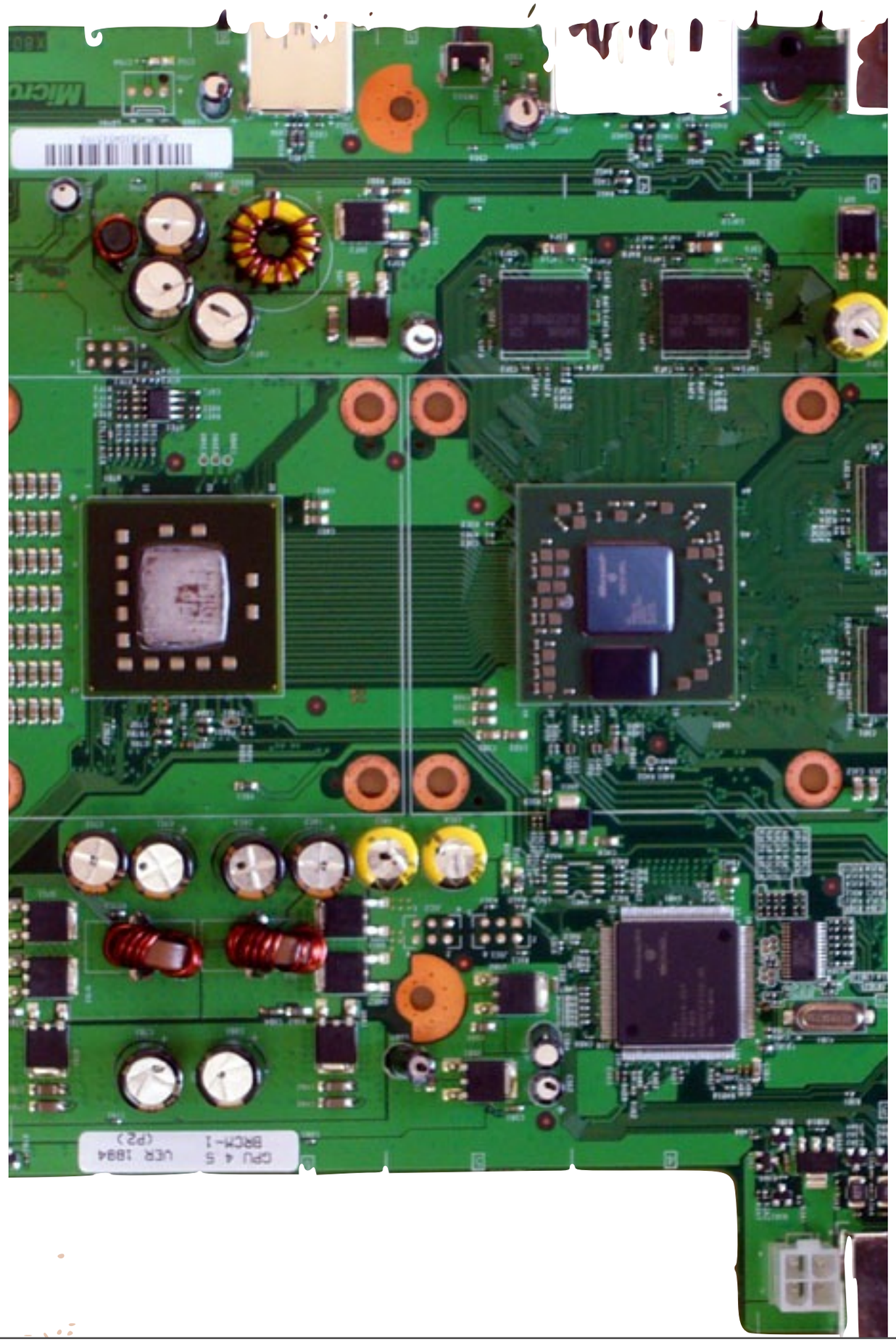
はじめに

- セキュリティに関しては、その性質上、完全な対応というものは存在しない。
- 記載のものに関しては、既知の対策による対応
- 今後、新たな攻撃 方法や手法、脆弱性が発覚した場合、都度その時点の最新バージョン、リビジョンを中心に対応を検討していく予定

iWP/iAF 7.x

の

セキュリティ対応



XSS対策

- スクリプト開発モデル
  - ＜IMART＞タグにエスケープ機能を追加
    - 画面共通 IMARTタグライブラリ
    - 画面デザイン共通 IMARTタグライブラリ

      上記2つ以外は順次対応予定

XSS対策

- スクリプト開発モデル
  - ＜IMART＞タグにエスケープ機能を追加
    - 画面共通 IMARTタグライブラリ
  - 画面デザイン共通 IMARTタグライブラリ

Ver.7.1.5で一部対応

Ver.7.2.3で一部対応

上記2つ以外は順次対応予定

XSS対策

- スクリプト開発モデル
  - ＜IMART＞タグにエスケープ機能を追加
    - 画面共通 IMARTタグライブラリ
  - 画面デザイン共通 IMARTタグライブラリ

上記2つ以外は順次対応予定

Ver.7.1.5で一部対応

Ver.7.2.3で一部対応

Ver. 7.2.3で対応

上記タグを使用して、ログイングループ管理者画面などの基盤側の

画面について、脆弱性対応を行った。（基盤側の全ての画面ではない）

XSS

- JavaEE開発モデル
- ポータル画面
- エラーページ
- BPW画面

XSS

- JavaEE開発モデル
- ポータル画面
- エラーページ
- BPW画面

Ver.7.1.6 以降対応予定

Ver.7.2.3で対応

HTTP Response Splitting

- iWP(Resin)では、HTTPレスポンスヘッダの改ざんを防ぐ仕組みがない。

- HTTPレスポンスヘッダやCookieを設定する際に、改行コードなど脆弱性に繋がる文字をサニタイズするFilterを提供

HTTP Response Splitting

Ver.7.1.5で対応

Ver.7.2.3で対応

- iWP(Resin)では、HTTPレスポンスヘッダの改ざんを防ぐ仕組みがない。

- HTTPレスポンスヘッダやCookieを設定する際に、改行コードなど脆弱性に繋がる文字をサニタイズするFilterを提供

システム情報の漏洩

- iWPが提供しているHTTPステータスコード「500」のエラーページ
  - 開発時の利用を目的としており、ページ内に発生した例外のスタックトレースが出力される。
  - スタックトレースに含まれる内容はシステムの秘密情報に当たる。
- スタックトレースの出力処理を取り除いたエラーページを提供

システム情報の漏洩

Ver.7.1.5で対応

Ver.7.2.3で対応

- iWPが提供しているHTTPステータスコード「500」のエラーページ
  - 開発時の利用を目的としており、ページ内に発生した例外のスタックトレースが出力される。
  - スタックトレースに含まれる内容はシステムの秘密情報に当たる。
- スタックトレースの出力処理を取り除いたエラーページを提供

ファイルアップロード機能の不備

- リクエストパラメータを改変し、画像ファイルと見せかけてJavaScriptを記載したテキストファイルをアップロードすることで、任意のスクリプトを実行できる。

- ファイルアップロードにチェック機能を追加（オプションでON/OFF可能）
  - アップロードされたファイルの拡張子が設定で許可されたものかチェック
    - 許可されていない拡張子はエラー
  - アップロードされたファイルの内容をチェック
    - ファイルの内容と拡張子が一致しない場合はエラー

ファイルアップロード機能の不備

- リクエストパラメータを改変し、画像ファイルと見せかけて JavaScriptを記載したテキストファイルをアップロードすることで、任意のスクリプトを実行できる。

Ver.7.1.5で対応

Ver.7.2.3で対応

- ファイルアップロードにチェック機能を追加（オプションでON/OFF可能）
  - アップロードされたファイルの拡張子が設定で許可されたものかチェック
    - 許可されていない拡張子はエラー
  - アップロードされたファイルの内容をチェック
    - ファイルの内容と拡張子が一致しない場合はエラー

CSRF対策

Webサイトにスクリプトや自動転送(HTTPリダイレクト)を仕込むことによって、閲覧者に意図せず別のWebサイト上で何らかの操作(掲示板への書き込みなど)を行わせる攻撃手法。

e-Words より

CSRF対策

Webサイトにスクリプトや自動転送(HTTPリダイレクト)を仕込むことによって、閲覧者に意図せず別のWebサイト上で何らかの操作(掲示板への書き込みなど)を行わせる攻撃手法。

Ver.7.1.6 以降対応予定

Ver.7.2.3 以降対応予定

e-Words より

IM-Workflow Ver.7.2

の

セキュリティ対応

セキュリティ対応

- XSS対策
- SQL Injection対策
- ディレクトリトラバーサル対策
- 攻撃のヒントを与える不要なコードの削除
  - HTMLコメント【作成者】などの削除
- hidden改変対策
- CSRF対策

セキュリティ対応

- XSS対策
- SQL Injection対策
- ディレクトリトラバーサル対策
- 攻撃のヒントを与える不要なコードの削除
  - HTMLコメント【作成者】などの削除
- hidden改変対策
- CSRF対策

Ver.7.2.4で対応

hidden改変対策

- ページ表示時に要求されたリクエストでアクセス権限があるかどうかを逐一チェックする。

- 逐一チェックできない項目については、キーがログイン毎に変化する暗号で暗号化を行ってから受け渡す。

CSRF対策

- 処理対象権限のチェック対象外のパラメータだけで情報参照を行っている画面
  - 暗号化コード (非可逆暗号) と非暗号化コードの相互チェックを行う。
- ログイングループID、ログインユーザIDを hidden パラメータとして渡さず都度セッションから取る。

Intranet Start Pack の

セキュリティ対応

セキュリティ対応

- XSS対策
- SQL Injection対策
- ディレクトリトラバーサル対策
- など

セキュリティ対応

- XSS対策

Ver.7.0.6で対応予定

- SQL Injection対策

Ver.7.1.2で対応予定

- ディレクトリトラバーサル対策

- など

続く

IMARTタグのエスケープ機能