Webサイトを守るためにわたしたちができること

EGセキュアソリューションズ株式会社
代表取締役 徳丸 浩

アジェンダ

- 最近の侵入事件に学ぶ
  - GMOペイメントゲートウェイのクレジットカート情報漏洩事件
  - 日本テレビの侵入事件
  - Drupageddon
  - Joomlaのコード実行脆弱性（CVE-2015-8562）
  - Joomla! の権限昇格脆弱性
- 今時のウェブサイトの守り方
  - 脆弱性情報公開から攻撃開始のますますの短時間化
  - 日本テレビ「個人情報不正アクセスに関する調査報告書」に学ぶ
- まとめ

Copyright © 2012-2017 EG Secure Solutions Inc.

徳丸浩の自己紹介

- 経歴
  - 1985年 京セラ株式会社入社
  - 1995年 京セラコミュニケーションシステム株式会社(KCCS)に出向・転籍
  - 2008年 KCCS退職、HASHコンサルティング株式会社（現EGセキュアソリューションズ株式会社）設立
- 経験したこと
  - 京セラ入社当時はCAD、計算幾何学、数値シミュレーションなどを担当
  - その後、企業向けパッケージソフトの企画・開発・事業化を担当
  - 1999年から、携帯電話向けインフラ、プラットフォームの企画・開発を担当
    Webアプリケーションのセキュリティ問題に直面、研究、社内展開、寄稿などを開始
  - 2004年にKCCS社内ベンチャーとしてWebアプリケーションセキュリティ事業を立ち上げ
- 現在
  - EGセキュアソリューションズ株式会社　代表　　http://www.eg-secure.co.jp/
  - 独立行政法人情報処理推進機構　非常勤研究員　　http://www.ipa.go.jp/security/
  - 著書「体系的に学ぶ 安全なWebアプリケーションの作り方」(2011年3月)
    「徳丸浩のWebセキュリティ教室 」(2015年10月)
  - 技術士（情報工学部門）

EG Secure Solutions

Copyright © 2012-2017 EG Secure Solutions Inc.

GMOペイメントゲートウェイのクレジットカード情報漏洩事件

Struts2 S2-045(CVE-2017-5638)

GMOペイメントゲートウェイに不正アクセス　クレジットカード情報など約72万件が流出した可能性

GMOペイメントゲートウェイが提供する決済サービスに不正アクセスがあり、東京都の都税クレジットカードお支払いサイトと、住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイトから、クレジットカードなどの情報約72万件が流出した可能性がある。

[園部修，ITmedia]

　GMOペイメントゲートウェイが3月10日、第三者による不正アクセスにより、クレジットカードの番号や有効期限などを含む71万9830件の情報が流出した可能性があると発表した。

　不正アクセスがあったのは、東京都の都税クレジットカード支払いサイトと、住宅金融支援機構の団体信用生命保険特約料クレジットカード支払いサイト。「Apache Struts2」の脆弱性を悪用した不正アクセスが発生し、悪意のあるプログラムが仕込まれていたことが判明した。調査の結果、クレジットカード番号やクレジットカードの有効期限、メールアドレスなどの情報が流出した可能性があることが分かった。

　なお現時点では、該当2サイト以外のサービスでは、同様の問題は発生していないことを確認しているという。

　不正アクセスの痕跡を確認したのは、3月9日の深夜。3月9日にIPAが発表した「Apache Struts2 の脆弱性対策について（CVE-2017-5638）（S2-045）」ならびにJPCERTの「Apache Struts 2の脆弱性（S2-045） に関する注意喚起」の情報に基づき、同日18時からGMOペイメントゲートウェイのシステムへの影響調査を行った結果判明した。Apache Struts 2の脆弱性対策はすでに実施済みだという。

http://www.itmedia.co.jp/enterprise/articles/1703/10/news157.html より引用

３．調査経緯と対策について

■3/9(木)

18:00
IPA独立行政法人情報処理推進機構様の「Apache Struts2 の脆弱性対策について(CVE-2017-5638)(S2-045)」（※1）ならびにJPCERT様の「Apache Struts 2 の脆弱性 (S2-045) に関する注意喚起」（※2）の情報に基づき、当社システムへの影響調査を開始。

20:00
当社内で当該脆弱の対象となるシステムの洗い出しが完了。対策方法の検討開始。

21:56
WAF（※3）にて該当する不正パターンによるアクセスの遮断を実施。[対策1]　同時に不正アクセスの可能性の調査を開始。

（※3）WAF（Web Application Firewall）Webサイト、およびその上で動作するWebアプリケーションを狙った攻撃を防御するセキュリティ対策システム。

23:53
不正アクセスの痕跡を確認したため「Apache Struts 2」が稼働しているシステムを全停止。ネットワーク未接続状態にあったバックアップシステムに切替を実施。[対策2]

https://corp.gmo-pg.com/news_em/20170310.html より引用

3．調査経緯と対策について

■3/10(金)

00:30

「Apache Struts 2」の脆弱性対策を[対策2]のバックアップシステムに実施。[対策3]

調査の結果、東京都様の都税クレジットカードお支払サイトと独立行政法人住宅金融支援機構様の団体信用生命保険特約料クレジットカード支払いサイトにおいて不正アクセスを確認。

02:15

東京都様の都税クレジットカードお支払サイトと独立行政法人住宅金融支援機構様の団体信用生命保険特約料クレジットカード支払いサイトにおいて不正にデータ取得された可能性が高いことを確認。

06:20

不正アクセスされた可能性のある情報の内容と件数を確認。

08:40～

東京都様の都税クレジットカードお支払いサイト運営会社ならびに独立行政法人住宅金融支援機構様へ報告。対策を協議。

https://corp.gmo-pg.com/news_em/20170310.html より引用

Apache Struts 2の脆弱性を突かれて不正アクセス、都税支払いサイトなどからクレジットカード情報72万件が流出した可能性

GMOペイメントゲートウェイ株式会社（GMO-PG）は10日、同社が運営受託している東京都税クレジットカード支払いサイトおよび独立行政法人住宅金融支援機構の団体信用生命保険特約料のクレジットカード支払いサイトに不正アクセスがあり、利用者のクレジットカード番号・有効期限など合計72万件近くの情報が流出した可能性があると発表した。アプリケーションフレームワーク「Apache Struts 2」の脆弱性「CVE-2017-5638/S2-045」を突かれたもの。

GMO-PGによると、いずれもクレジットカード番号は暗号化処理された状態だったという。一方、住宅金融支援機構のサイトにおいては、クレジットカード番号・有効期限のほか、セキュリティコード、住所、氏名、電話番号、生年月日なども含まれている。セキュリティコードの情報は、カード業界のセキュリティ標準であるPCI DSSによりシステムで保持してはならないことになっているが、今回の不正アクセス被害で調査するまで、セキュリティコードを保持していることをGMO-PGでは認識していなかったとしている。

CVE-2017-5638/S2-045の脆弱性については、脆弱性を修正したバージョン「2.3.32」および「2.5.10.1」がリリース済みだが、これを狙った攻撃が3月7日ごろから急増していることがセキュリティベンダー各社から報告されていた。これを受けてGMO-PGが9日、この脆弱性の対象となる同社のシステムの洗い出しを行ったところ、上記2サイトに悪意あるプログラムが仕掛けられ、第三者に不正にデータを取得された可能性が高いことが判明した。詳細はフォレンジック調査中だが、日本時間の8日未明に不正アクセスされた痕跡が確認されており、その時点でプログラムが仕掛けられたとみられる。

http://internet.watch.impress.co.jp/docs/news/1049261.html より引用

時系列のまとめ（日本時間）

3月6日 19時頃	S2-045のアドバイザリー公開、修正バージョンが dev リポジトリにUPされる、
3月7日 21時頃	修正バージョンが dev から release に移される
3月7日 20時頃	JP-Secure SiteGuardシリーズのWAFにてS2-045対応のシグネチャを配信
3月8日 早朝	東京都税クレジットカード支払いサイトおよび団体信用生命保険特約料のクレジットカード支払いサイト（以下、両サイト）に不正アクセス（後に判明）
3月8日 午後	IPAから注意喚起
3月8日 21時頃	正式アナウンスのメール、Webサイト更新
3月9日 午前	JPCERT/CCから注意喚起
3月9日 18:00	GMO-PGにてS2-045を把握、対象サイトの洗い出しを開始
3月9日 20:00	対象となるシステムの洗い出しが完了、対策方法の検討開始
3月9日 21:56	WAFにシグネチャを設定
3月9日 23:53	不正アクセスの痕跡を確認したため「Apache Struts 2」が稼働しているシステムを全停止。ネットワーク未接続状態にあったバックアップシステムに切替を実施
3月10日 00:30	両サイトにおいて不正アクセスを確認
3月10日 02:15	両サイトにおいて不正にデータ取得された可能性が高いことを確認。

https://twitter.com/kitagawa_takuji/status/839457500021702660
http://internet.watch.impress.co.jp/docs/news/1049261.html
https://corp.gmo-pg.com/news_em/20170310.html などをもとにまとめた

Struts2 S2-045の攻撃はどうすれば防げたか? or 緩和できたか?

- 早期に脆弱性情報をキャッチして以下のいずれかを行う
  - とにかく パッチ適用 / バージョンアップをやってしまう
  - サイトを停止する
- 高性能のWAFを導入する
- データを暗号化する
  - Internet Watchの記事によると、両サイトともクレジットカード番号は暗号化された状態で保存されていた
  - 4月14日付けのリリースで、不正利用は確認されていないとのこと
- ファイルパーミッションの制限
- SELinuxの活用
- いわゆる"出口対策" として外向き通信の制限

Copyright © 2012-2017 EG Secure Solutions Inc.

日本テレビの侵入事件

ケータイキット for Movable Type

Copyright © 2012-2017 EG Secure Solutions Inc.

ニュース

日経コンピュータ

J-WAVEでも64万件の個人情報流出の可能性、原因ソフトの利用者は至急パッチ適用を

2016/04/23
井上 英明＝日経コンピュータ （筆者執筆記事一覧）

記事一覧へ >>

373 シェア
51 ブックマーク
53 Pocket
ツイート
保存する

J-WAVEは2016年4月22日、Webサイトへの不正アクセスにより、リスナーなどの個人情報約64万件を流出させた可能性があると公表した。原因はアイデアマンズ製「ケータイキット for Movable Type」の脆弱性で、同社は22日にパッチファイルを公開した。既に攻撃が成功しているため、同ソフトの利用者はパッチを至急適用する必要がある。

流出した可能性がある個人情報は、名前や住所、メールアドレス、電話番号、性別、年齢、職業など約64万件。2007年以降にJ-WAVEのWebサイトから番組あてに送ったメッセージやプレゼント応募者のデータという。「2006年以前のデータは保存期間を過ぎているため消去済みだった」（J-WAVE広報）。

http://itpro.nikkeibp.co.jp/atcl/news/16/042301210/ より引用

ケータイキット for Movable Type の脆弱性 (CVE-2016-1204) に関する注意喚起

各位

JPCERT-AT-2016-0019
JPCERT/CC
2016-04-26(新規)
2016-05-06(更新)

<<< JPCERT/CC Alert 2016-04-26 >>>
ケータイキット for Movable Type の脆弱性 (CVE-2016-1204) に関する注意喚起
https://www.jpcert.or.jp/at/2016/at160019.html

I. 概要

アイデアマンズ株式会社のケータイキット for Movable Type には、OS コマンドインジェクションの脆弱性 (CVE-2016-1204) があります。この脆弱性を悪用された場合、当該製品が動作するサーバ上で任意の OS コマンドを実行される可能性があります。

本脆弱性や影響の詳細については、以下を参照してください。

Japan Vulnerability Notes JVNVU#92116866
ケータイキット for Movable Type に OS コマンドインジェクションの脆弱性
https://jvn.jp/vu/JVNVU92116866/

なお、本脆弱性を悪用した攻撃活動が確認されているとの情報があります。

https://www.jpcert.or.jp/at/2016/at160019.html より引用

日本テレビ 個人情報不正アクセスに関する調査報告書 より引用

1　技術的観点からの調査結果

(1)　攻撃に関するログ調査

本件事故は、A 社が提供するモバイルサイトを構築するソフトウェアのケータイキットが設置されたウェブサーバ（以下「本件システム」という。）に対するサイバー攻撃によるものであった。本委員会にて入手したログより、攻撃内容を調査した結果、攻撃は以下の 3 種類の段階によって実施されたことが判明した。

① ケータイキット最新版（v1.641）における OS コマンドインジェクションの未知の脆弱性を利用し、本件システムへ遠隔操作プログラムを設置

② 本件システム上の遠隔操作プログラムを操作して、本件システム内部を探索

③ 本件システムから個人情報データを外部に不正持ち出し

http://www.ntv.co.jp/oshirase/20160714.pdf

ケータイキット for Movable Typeは何が問題だったか?

- ImageMagickのconvertコマンドを用いて画像変換をしている
  # わりとよくある
- convertコマンドのパラメータについて
  - バリデーションを十分していない
  - エスケープもしていない ← こちらが主原因
- ファイル名については、ファイルの存在チェックがあり、攻撃は難しい
- convertに渡すパラメータはノーチェック
- OSコマンドインジェクションが可能

Copyright © 2012-2017 EG Secure Solutions Inc.

Drupageddon

DruaplのSQLインジェクション脆弱性(CVE-2014-3704)

Copyright © 2012-2017 EG Secure Solutions Inc.

Drupalとは

Drupal（ドルーパル、発音: /ˈdruːpəl/）は、プログラム言語PHPで記述されたフリーでオープンソースのモジュラー式フレームワークであり、コンテンツ管理システム (CMS) である。昨今の多くのCMSと同様に、Drupalはシステム管理者にコンテンツの作成と整理、提示方法のカスタマイズ、管理作業の自動化、サイトへの訪問者や寄稿者の管理を可能にする。

その性能がコンテンツ管理から、幅広いサービスや商取引を可能にするにまで及ぶことから、Drupalは時々「ウェブアプリケーションフレームワーク」であると評される。Drupalは洗練されたプログラミング・インターフェースを提供するものの、基本的なウェブサイトの設置と管理はプログラミングなしに成し遂げることができる。Drupalは一般に、最も優れたWeb 2.0フレームワークの一つであると考えられている。

※Wikipediaより引用

WhiteHouse

NASA

国立国会図書館カレントアウェアネス

https://ja.wikipedia.org/wiki/Drupal より引用

Drupageddon(CVE-2014-3704)とは

- Drupal Ver7.31以前に存在するSQLインジェクション脆弱性
- 非常に危険性の高い脆弱性であるので、アルマゲドンをもじってドゥルパゲドンと命名された模様
- Drupal core の データベース抽象化 API （一種のSQLジェネレータ）の expandArguments 関数における SQL インジェクションの脆弱性
- 日本ではあまり話題になっていない（Drupalのシェアのせい?）

Copyright © 2012-2017 EG Secure Solutions Inc.

Drupalの脆弱性突く攻撃横行、「侵入されたと想定して対処を」

オープンソースのコンテンツ管理システム（CMS）「Drupal」に極めて深刻な脆弱（ぜいじゃく）性が見つかった問題で、Drupalは10月29日、脆弱性修正のパッチを直後に適用しなかったWebサイトは侵入された可能性があると警告した。米セキュリティ機関のUS-CERTも、アップデートや回避策の適用を呼びかけている。

問題のSQLインジェクションの脆弱性は、Drupalのバージョン7.xに存在する。悪用された場合、攻撃者にバックドアを仕掛けられ、サイトの全データをコピーされる恐れがある。攻撃の痕跡は残らない。この脆弱性を修正した「Drupal 7.32」は10月15日にリリースされた。

Drupalによると、この10月15日の発表の直後から、脆弱性を修正していないWebサイトに対する攻撃が始まった。「すべてのDrupal 7サイトは、世界協定時間の10月15日午後11時（日本時間16日午前8時）までにアップデートまたはパッチを適用していない限り、破られたと想定して対処しなければならない」とDrupalは警告する。

http://www.itmedia.co.jp/enterprise/articles/1410/31/news050.html より引用

えのしま・ふじさわポータルサイト（えのぽ） 侵入事件

Joomlaのコード実行脆弱性（CVE-2015-8562）

Copyright © 2012-2017 EG Secure Solutions Inc.

「Joomla！」脆弱性を突かれスパム送信の踏み台に - 藤沢市関連サイト

「えのしま・ふじさわポータルサイト（えのぽ）」が不正アクセスを受け、スパムメール送信の踏み台に悪用されていたことがわかった。

同サイトは、藤沢市が開設し、その後NPO法人である湘南ふじさわシニアネットが藤沢市と協働運営の協定のもと運営する地域のポータルサイト。藤沢市によれば、同サイトで利用するコンテンツマネージメントシステム（CMS）の「Joomla！」とPHPの既知の脆弱性が突かれ、不正アクセスを受けたという。

2015年12月24日にサーバの負荷が急増したことからサーバを停止。1月12日より同市が調査を行っていたが、今回の不正アクセスにより、同サーバより約60万件のスパムメールが送信されていたことが判明した。

同サイトでは、「健康づくり応援団」「おいしいふじさわ産」「いきいきシニアライフ」「自治会・町内会ページ」などのコンテンツも運営しているが、いずれも個人情報を扱っておらず、情報漏洩はないと説明している。

同サイトは現在も停止しており、セキュリティ対策など再発防止策を講じたうえで再開する予定。

http://www.security-next.com/066075 より引用

Joomlaに深刻な脆弱性、パッチ公開2日前から攻撃横行

セキュリティ企業によると、Joomlaの脆弱性修正パッチが公開される2日前から、この脆弱性を突くゼロデイ攻撃の発生が確認されていたという。

　オープンソースのコンテンツ管理システム（CMS）「Joomla」の更新版が12月14日（米国時間）に公開され、深刻な脆弱性が修正された。セキュリティ企業のSucuriは、パッチが公開される2日前からこの脆弱性を突くゼロデイ攻撃の発生が確認されていたとして、Joomlaを使っているWebサイトでは直ちにパッチ適用やログ確認などの対応に乗り出すよう促している。

　Joomlaの脆弱性はバージョン1.5.0～3.4.5に存在していて、悪用されればリモートでコードを実行される恐れがある。更新版のバージョン3.4.6でこの問題が修正された。

　Sucuriのブログによれば、この脆弱性は簡単に悪用することができるといい、12月12日の時点で既に、この問題を悪用した攻撃コードが出回っていたという。

　同月13日から14日にかけて攻撃はさらに拡大。Sucuriが運営するWebサイトやハニーポットがことごとく攻撃されたといい、「他のあらゆるJoomlaサイトも恐らく標的になっている」と同社は推測する。

http://www.itmedia.co.jp/enterprise/articles/1512/15/news048.html より引用

攻撃の方法（ネットで流通しているものを一部改変）

- User-Agentに下記を設定してJoomla!サイトに2回アクセスするだけ。かんたん!

}__test|O:21:"JDatabaseDriverMysqli":3:{s:2:"fc";O:17:"JSimplepieFactory":0:{}s:21:"¥0¥0¥0disconnectHandlers";a:1:{i:0;a:2:{i:0;O:9:"SimplePie":5:{s:8:"sanitize";O:20:"JDatabaseDriverMysql":0:{}s:8:"feed_url";s:239:"eval(chr(115).chr(121).chr(115).chr(116).chr(101).chr(109).chr(40).chr(39).chr(116).chr(111).chr(117).chr(99).chr(104).chr(32).chr(47).chr(116).chr(109).chr(112).chr(47).chr(102).chr(120).chr(39).chr(41).chr(59));JFactory::getConfig();exit";s:19:"cache_name_function";s:6:"assert";s:5:"cache";b:1;s:11:"cache_class";O:20:"JDatabaseDriverMysql":0:{}}i:1;s:4:"init";}}s:13:"¥0¥0¥0connection";b:1;}
吉野家

Copyright © 2012-2017 EG Secure Solutions Inc.

攻撃の流れ(Sucuriの解説より)

- Joomla! がUser-Agentをセッション変数に保存するので、セッション形式のデータ（文字列）をUser-Agent経由でセットする
- その際、「吉野家」がトリガーとなって、セッションデータの切り詰めが起きる（MySQLの仕様）
- 切り詰めが起きると、文字列がオブジェクトに化ける（PHPの脆弱性CVE-2015-6835PHPの脆弱性 ）
- 生成されたオブジェクトのデストラクタ経由にて任意のスクリプト実行が可能になる

Copyright © 2012-2017 EG Secure Solutions Inc.

Joomla! の権限昇格脆弱性
CVE-2016-8869、CVE-2016-8870

Copyright © 2012-2017 EG Secure Solutions Inc.

CVE-2016-8869等はどのような問題か?

- どのような問題か?
  - ユーザー登録時に、管理者権限を設定されてしまう(CVE-2016-8869)
  - ユーザー登録を許可していない設定でもユーザー登録ができてしまう(CVE-2016-8870)
- なにが原因だったか?
  - Joomla!内にユーザー登録のメソッドが2つ存在した
    - UsersControllerRegistration::register()
    - UsersControllerUser::register()
  - UsersControllerUser::register() の方は、ユーザー登録許可の設定を確認していない!
  - 同じく、外部から権限を示すコードを設定可能
  - UsersControllerUser::register()を外部から呼び出す経路が存在した
- どう対策したか?
  - UsersControllerUser::register()の削除
- 利用者はどうすればよいか?
  - Joomla!のバージョンアップ

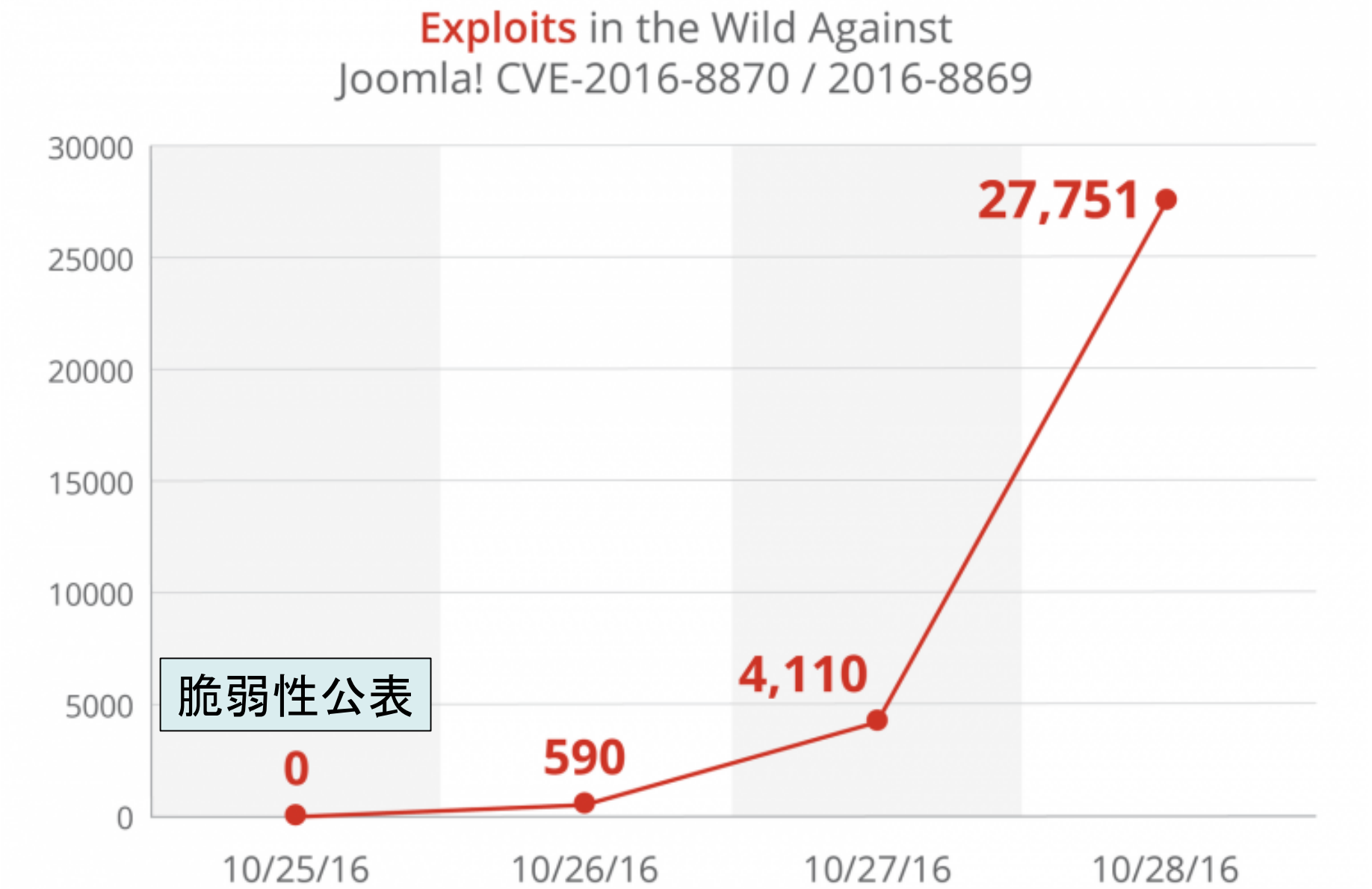
Copyright © 2012-2017 EG Secure Solutions Inc.

CVE-2016-8869等から得られる教訓

- 使わなくなったコードは速やかに削除しよう
- 脆弱性診断の古典的な観点ではあるが…
  - ソースを追わないと判らない場合が多い
  - 内部構造を熟知していないと、短期間の脆弱性診断では指摘できない
- 脆弱性診断で、「使わないコードを削除する」ように勧めている理由
  - 古いコードには脆弱性があるかもしれない
  - 拡張を.bak等に変更しているとソースコードが閲覧できてしなう
  - デバッグ機能等の場合は、バックドアとして悪用される可能性
- 「古いコード」がこれほどまでに「悪用可能」な例は珍しく、ちょっと興奮した　← 違法ではないが一部不適切
- やはり、古いコードは速やかに削除しよう

Copyright © 2012-2017 EG Secure Solutions Inc.

Joomla!の脆弱性 CVE-2016-8869等の攻撃検知数推移



https://blog.sucuri.net/2016/10/joomla-mass-exploits-privilege-vulnerability.html より引用

今時のウェブサイトの守り方

Copyright © 2012-2017 EG Secure Solutions Inc.

脆弱性対処の"猶予期間"はますます短くなる

- Drupal　CVE-2014-3704　公表の数時間後
- KeitaiKit　CVE-2016-1204　ゼロデイ
- Joomla!　CVE-2015-8562　ゼロデイ
- Joomla!　CVE-2016-8869　公表の翌日
- WordPress　CVE-2017-1001000　情報公開の48時間以内
- Struts2　CVE-2017-5638　ゼロデイ（正式バージョンアップの前）

- 攻撃者は、脆弱性情報公表を待ち構えている
- サイト運営者も同様の備えを

Copyright © 2012-2017 EG Secure Solutions Inc.

CMS「Joomla!」に危険度の高い脆弱性、直ちに最新版へのアップデートを

オープンソースのコンテンツ管理システム（CMS）「Joomla!」に危険度の高い脆弱性が存在するとして、開発元のコミュニティは25日、脆弱性を修正した最新版となる「バージョン3.6.4」を公開した。開発コミュニティでは、直ちにアップデートを行うことを強く推奨している。

　修正した脆弱性は、アカウントの作成が可能となる「CVE-2016-8870」と、特権の昇格が可能となる「CVE-2016-8869」の2件。いずれも、Joomla!のバージョン3.4.4から3.6.3までに影響がある。このほか、二要素認証に関する修正も行われている。

　Joomla!の開発コミュニティでは、重要なセキュリティ修正を公開することを10月21日に公表し、ユーザーにアップデートの準備を促していた。また、今回のアップデートは、セキュリティ修正とバグ修正のみで、他の修正は行われていないとして、ユーザーに対して最新版へのアップデートを強く推奨している。

http://internet.watch.impress.co.jp/docs/news/1026829.html より引用

日頃から最新版に追随していないと、イザという時に困る

- 先の記事で、“今回のアップデートは、セキュリティ修正とバグ修正のみで、他の修正は行われていない” という箇所は、機能追加等はしていないので、バージョンアップの悪影響は極力排除した、という意味
- しかし、その恩恵を享受するためには、Joomla!の最新版が導入されていないと意味がない
  - Joomla! 3.6.3 → Joomla! 3.6.4　（バグ修正のみ）　影響は軽微
  - Joomla! 3.4.1 → Joomla! 3.6.4　（機能追加含む）　影響を受ける可能性が増える
- つまり、さしせまった脆弱性等がなくても、ソフトウェアを最新版にしておかないと、火急の脆弱性が公表された場合にバージョンアップを躊躇する要因となる

Copyright © 2012-2017 EG Secure Solutions Inc.

「個人情報不正アクセスに関する調査報告書」から

第３　本件事故の原因調査

本件事故は、フォアキャストが、ウェブシステムの未知の脆弱性を突く攻撃を受けたことに起因して、個人情報が外部に送信されたものであり、その直接の原因は、未知の脆弱性という一見不可避とも思える偶発的な事象であった。もっとも、未知の脆弱性という点を措いても、その他の情報セキュリティ施策が有効に機能していれば避けられた事故であったともいえる。そこで、以下では、まず、本件事故の原因調査として、フォアキャストのウェブシステムの情報セキュリティに関し、技術的観点に基づく検証をするとともに、NTV 及びフォアキャストにおける個人情報の管理体制についても検証した。

「個人情報不正アクセスに関する調査報告書」より引用
http://www.ntv.co.jp/oshirase/20160714.pdf

「個人情報不正アクセスに関する調査報告書」から（続き）

A)侵入を検知・防御する対策（入口対策）

①ツールによる脆弱性診断を約2年前に実施済みであった。しかし、今回の攻撃に悪用された脆弱性は、当該診断時には発見できなかった。また、上記時点以降は脆弱性診断を実施していない。

②IDS（不正侵入検知システム）を導入しており、常時監視をしていた。しかし、今回のOSコマンドインジェクションは検知できなかった。

③不要なウェブリクエストがプログラム上で制限されていなかった。

④プログラム言語の設定として不要な呼び出し関数の実行が制限されていなかった。

⑤ファイルが不要に設置されたことを検知する仕組みがなかった。

⑥プログラムが動作する範囲が適切でなかった。

「個人情報不正アクセスに関する調査報告書」より引用
http://www.ntv.co.jp/oshirase/20160714.pdf

「個人情報不正アクセスに関する調査報告書」から（続き）

B)侵入された後に情報の探索・流出を防ぐ対策（内部対策、出口対策）

①サーバー上に不要なプログラムが残っていた。

②ウェブサーバーのアカウントで、サーバー上のデータに自由にアクセスできていた。

③ウェブサーバから個人情報データが保存されたディスクが直接マウントされ閲覧操作できる状態にあった。なお、ウェブサーバに不正侵入しない限り、インターネット側から当該ディスクにアクセスすることはできなかった。

④個人情報データは、暗号化されておらず、平文で保存されていた。

⑤削除すべき過去の個人情報データがディスクに残っていた。

⑥個人情報データが保存されていることを推測されやすいファルダ名を利用していた

⑦サーバのネットワーク設定が実装されていなかった

⑧ウェブサーバから外部への通信が全て許可されていた

「個人情報不正アクセスに関する調査報告書」より引用
http://www.ntv.co.jp/oshirase/20160714.pdf

ケータイキットのゼロデイ脆弱性はどうすれば防げたか?

- WAFの使用…高性能なWAFならば検出できた可能性
- 不要な関数の制限…ケータイキットの実装には、OSコマンド呼び出しの関数(exec)が使用されており、制限できない
- 改ざん検知…改ざん検知システムによりWebShellの設置を早期に検知すれば、侵入を早期に察知して、被害を最小限にできた可能性
- ウェブサーバーのアカウントの権限抑止…一般的に有効だが、アプリケーションが個人情報を扱う以上限界がある
  - ケータイキットはPHPスクリプトを設置するディレクトリに画像ファイルをアプリケーションが書き込むので、パーミッション制限が難しい
- 個人情報の暗号化…有効だが、鍵の保存方法に課題
- 外部への通信の制限…課題はあるが、少なくとも時間稼ぎにはなった可能性

Copyright © 2012-2017 EG Secure Solutions Inc.

各脆弱性はWAFで防御できたか?

- Drupal　CVE-2014-3704　防御可
- KeitaiKit　CVE-2016-1204　防御可
- Joomla!　CVE-2015-8562　防御可
- Joomla!　CVE-2016-8869　△（カスタマイズ要）
- WordPress REST API　防御可（専用シグネチャ）
- Struts2　CVE-2017-5638　防御可（専用シグネチャ）

- SQLインジェクション、OSコマンドインジェクション等は、WAFの標準シグネチャで防御できる可能性が高いので、ゼロデイ脆弱性にも効果が見込める

Copyright © 2012-2017 EG Secure Solutions Inc.

Webサイトを守るためにわたしたちができること

- まずは基本の施策を
  - 脆弱性の排除
  - ログインを強固に
- パッチ適用し易い環境を作る（パッチ適用容易性の確保）
  - パッチ適用等を作る見越したプラットフォーム選定を
  - 緊急性がなくても、バージョンアップを行っておく
- 追加の防御施策で多層防御を
  - ファイルパーミッションの制限
  - SELinuxの導入、設定
  - WAFの導入
  - 改ざん検知システムによる早期検知と対策

Copyright © 2012-2017 EG Secure Solutions Inc.