Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年 12 月 30 日

Topic

PHP の脆弱性を標的とした不正なアクセスの観測について

「Joomla!」を使用したウェブサイトに対するPHPの脆弱性を標的とした不正なアクセスを観測しました。PHP を利用している全てのサイト管理者は速やかな対策を実施することを推奨します。

1 今回判明した重大な脆弱性について

「Joomla!」は多くのウェブサイトの構築・運用に利用されているコンテンツ管理システム（CMS）です。12 月 14 日に、この「Joomla!」において任意の PHP コードが実行可能となる重大な脆弱性が公表[i]され、開発元から修正版がリリースされました。

また、21 日には開発元から当該脆弱性の根本的な原因は、PHP における既知の脆弱性によるものであったことが公表[ii]されています。このことから、ウェブサイトに「Joomla!」を使用していない場合においても、PHP を使用している場合は、攻撃者によって、遠隔から任意のコードを実行される危険性があります。

2 観測状況について

当該脆弱性の公表後、12 月 14 日にセキュリティ対策企業から「Joomla!」を使用したウェブサイトに対する PHP の脆弱性を標的とした不正なアクセスの観測事例が公表[iii]されました。また、24 日には別のセキュリティ対策企業からも同様の事例が公表[iv]されました。

警察庁の定点観測システムにおいても 28 日にこれらのセキュリティ対策企業から公表されたアクセスと同様の手法によるアクセスを観測しました（図1）。

[i] https://www.joomla.org/announcements/release-news/5641-3-4-6-released.html
https://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-vulnerability.html
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-006456.html
[ii] https://www.joomla.org/announcements/release-news/5643-joomla-3-4-7.html
[iii] https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html
[iv] http://www.symantec.com/connect/blogs/joomla

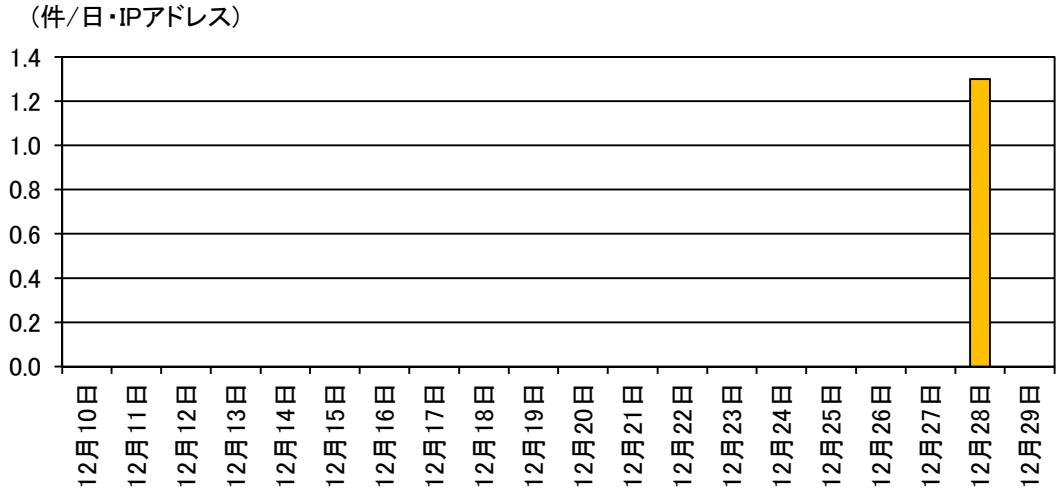

図1 「Joomla!」を使用したウェブサイトに対する PHP の脆弱性を標的とした不正なアクセス件数の推移（10 日～29 日）

これらアクセスの内容は、いずれも脆弱性の有無を確認するものであり、実際に攻撃を試みるアクセスではありませんでした（図2）。

```
GET /joomla/ HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: }__test|O:21:"JDatabaseDriverMysqli[redacted]
[redacted]
[redacted]phpinfo()[redacted]
[redacted]
[redacted]
[redacted]
```

図2 観測したアクセス内容（内容の一部についてはマスキングを実施）

しかしながら、このアクセスにより脆弱性が存在することが判明したウェブサーバに対しては、今後、さらに当該脆弱性を悪用する攻撃が実施され、サイトの改ざん等が発生する危険性もあるため、十分注意が必要です。

3 推奨する対策

今回の問題の根本的な原因は PHP に存在するため、「Joomla!」に限らず、PHP を利用している全てのサイト管理者は、PHP を最新のバージョンにアップデートすることを推奨します。

また、「Joomla!」を利用するウェブサイトにおいて、PHP のアップデートを直ちに実施することが困難な場合には、「Joomla!」を最新のバージョンにアップデートすることで、今回判明

した「Joomla!」を悪用する不正なアクセスを防止することは可能とされています。しかしながら、今後、「Joomla!」以外を攻撃の糸口として PHP の脆弱性を狙った攻撃を受ける可能性もありますので、あくまでも一時的な緩和策であることに留意する必要があります。