GNU bash の脆弱性に関する注意喚起

rev1.1

平成 26 年 10 月 1 日

株式会社ファイブドライブ
〒100-0011 東京都千代田区内幸町 1-1-7
TEL:03-5511-5875/FAX:03-5512-5505

注意事項

本文書は2014年9月30日時点で公開されている脆弱性情報にもとづいて作成されています。脆弱性の影響を受ける条件、改善策及び回避策等は公開情報をもとに記載しており、今後新たに公開される情報により変更される可能性がありますのでご注意ください。

目　次

1. 脆弱性の概要

Red Hat Enterprise LinuxやCentOSなど、Linux系OS等で利用されているGNU bashにおいて、不正にコマンドが実行可能な脆弱性が報告されました。

CVE	CVE-2014-6271 (CVSS基本値10.0) CVE-2014-7169 (CVSS基本値10.0) CVE-2014-7186 (CVSS基本値10.0) CVE-2014-7187 (CVSS基本値10.0) CVE-2014-6277 (CVSS基本値10.0) CVE-2014-6278 (CVSS基本値:未評価)
リモートからの攻撃の可否	可
攻撃コード（攻撃手法）の公開	公開済み

2. 影響するソフトウェア・バージョン

- bash 4.3 Patch 26 及びそれ以前のバージョン
- bash 4.2 Patch 49 及びそれ以前のバージョン
- bash 4.1 Patch 13 及びそれ以前のバージョン
- bash 4.0 Patch 40 及びそれ以前のバージョン
- bash 3.2 Patch 53 及びそれ以前のバージョン
- bash 3.1 Patch 19 及びそれ以前のバージョン
- bash 3.0 Patch 18 及びそれ以前のバージョン

本脆弱性はbashの環境変数の処理に起因する問題ですが、以下のソフトウェアを利用している場合にリモートおよびローカルから影響を受ける可能性があります（※についてはインターネット経由で影響を受ける可能性があります)。

- OpenSSH（※）
- httpd（Apache HTTP Server）（※）
- mod_cgi（※）
- mod_cgid（※）
- dhclient
- sudo（SUIDにより権限が設定されたプログラム）
- postfix
- CUPS

- Firefox（拡張機能、アドオン使用時）

※ 以下のソフトウェアは、本脆弱性の影響を受けません。

- mod_php
- mod_python
- mod_perl

3. 想定されるリスク

動作しているソフトウェアとその設定にもよりますが、リモートから任意のコマンドを実行される可能性があります。特に、Web サーバにおいて CGI の実行によるサービスを提供していて、かつ、CGI プログラム内部で bash を呼び出している場合には、インターネット経由での攻撃が比較的容易な状態となります。

4. 脆弱性の詳細

GNU bash には環境変数にシェルの関数を定義し、他のシェルプロセスで定義したシェル関数を実行する機能があります。GNU bash には環境変数に定義されたシェル関数の処理に不備があり、関数定義に引き続きシェルコマンドが記述されていると、関数定義を取り込む際にシェルコマンドが実行されます。

上記で言及した CGI プログラムの実行に際しては、Web ブラウザやアクセス元 URL の情報が環境変数を通じて Web サーバから CGI プログラムに引き渡される仕組みとなっています。そのため、インターネット経由での攻撃が容易です。

5. 脆弱性の有無の確認方法

確認を実施したいサーバで以下のコマンドを実行してください。($はコマンドプロンプト)

※CVE-2014-6271 を確認する場合の方法です。他の CVE を確認する場合には参考情報をご確認ください。

```
$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

以下のような出力となった場合には**脆弱性が存在します。**

```
vulnerable
this is a test
```

以下のような出力となった場合には**脆弱性は存在しません。**

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
this is a test
```

6. 改善策

脆弱性発表直後に提供された「CVE-2014-6271」「CVE-2014-7169」に対して製品(OS)提供ベンダ及び bash 開発元の GNU プロジェクトからアップデートパッケージやパッチが提供されましたが、対策漏れがあることが確認されています。さらなる対応として、一部の製品(OS)提供ベンダから「CVE-2014-7186」「CVE-2014-7187」を修正するアップデートパッケージやパッチが提供されています。なお、現時点では「CVE-2014-6277」「CVE-2014-6278」に対応するパッチは提供されていません。

現在提供されている bash の最新のバージョンは以下の通りです。（CVE-2014-6271、CVE-2014-7169 のみ修正されています）

- bash 4.3 Patch 27 及びそれ以前のバージョン
- bash 4.2 Patch 50 及びそれ以前のバージョン
- bash 4.1 Patch 14 及びそれ以前のバージョン
- bash 4.0 Patch 41 及びそれ以前のバージョン
- bash 3.2 Patch 54 及びそれ以前のバージョン
- bash 3.1 Patch 20 及びそれ以前のバージョン
- bash 3.0 Patch 19 及びそれ以前のバージョン

ご利用の製品(OS)ベンダから、各 CVE 番号の脆弱性に対応したアップデートパッケージやパッチが提供されている場合には、適用を行ってください。「CVE-2014-6271」のみなど、一部の脆弱性のみを修正するアップデートパッケージやパッチのみが提供されている場合は、パッケージのアップデートやパッチの適用を行うと共に、下記の回避策の適用を行ってください。

7. 回避策

改善策の実施が困難な場合は、一時的な回避策として以下の方法を 1 つ以上実施することが挙げられます。

- GNU bash をその他のシェルに入れ替える
- WAF や IPS を用いて脆弱性のあるサービスへの入力をフィルタする

※ 回避策は一時的に脆弱性の影響を回避することを目的としたものであり、本脆弱性によるすべての攻撃を防御できることを保証するものではありません。回避策の実施と同時に改善策の実施を進めることを推奨いたします。

8. 参考情報

- JPCERT「GNU bashの脆弱性に関する脆弱性」
  http://www.jpcert.or.jp/at/2014/at140037.html
- IPA/JVN「GNU BashにOSコマンドインジェクションの脆弱性」
  http://jvn.jp/vu/JVNVU97219505/
- IPA「bashの脆弱性対策について（CVE-2014-6271 等）」
  https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html
- Bash Code Injection Vulnerability via Specially Crafted Environment Variables (CVE-2014-6271, CVE-2014-7169)
  https://access.redhat.com/articles/1200223
- demonstration of CVE-2014-7186 ShellShock vulnerability
  https://lists.gnu.org/archive/html/bug-bash/2014-09/msg00238.html

本文書の記載内容についてご不明な点がございましたら、下記のお問い合わせ先までお問い合わせください。

株式会社ファイブドライブ
TEL：03-5511-5875（受付時間：平日 10 時～18 時）
FAX：03-5512-5505
MAIL：secinfo@fivedrive.jp
担当：脆弱性情報担当

以上