Openfind
安全性程式更新手冊

網擎資訊軟體股份有限公司 謹呈
Openfind Information Technology, Inc.

2014.09.25

前言

在 UNIX 平台上被廣泛使用的 Bash Shell 含有嚴重漏洞 (CVE-2014-6271)，可讓駭客遠端執行惡意程式，影響 GNU、Linux 及 Mac OS X 等 UNIX-Like 的各種作業系統。Bash Shell 是一個非常廣泛被應用的殼層程式，它採用命令列介面，允許使用者輸入文字命令，也可讓使用者遠端下達指令 (如透過 SSH 或 Telnet)。

Openfind 資安團隊接獲通知後，立即調查受影響的產品範圍，發現雖然此次受影響的範圍包含到所有使用 Bash 的 UNIX-Like 系統，但是修正並不會太困難，只需要根據此份文件的**檢測方法**與**修補方法**，便可透過簡單的步驟，完成檢查與更新。

P.S.： 特別提醒使用者，此漏洞是 UNIX-Like 系統 Bash Shell 本身的問題，建議貴單位全面徹查所有 UNIX-Like 的系統，並透過相同方式進行檢測及更新，以確保企業的資訊安全。

檢測方法

由於各系統版本不同，所呈現的檢測結果也會不同，請參考下列兩種檢測方式，當檢測結果與文件所述有差異時，請使用另一種方法檢測。

檢測方法一：

1. 在 Shell 中輸入下列指令

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

2. 依照系統回應資訊判斷是否需要更新

2.1. 若系統回應以下資訊，則表示**需要更新您的系統**

```
Vulnerable
this is a test
```

實際畫面請參考：

```
[root@modify-me ~]# bash --version
GNU bash, version 4.1.2(1)-release (i386-redhat-linux-gnu)
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
[root@modify-me ~]# x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
[root@modify-me ~]#
```

2.2. 若系統回應以下資訊，則表示**不需要更新您的系統**

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

實際畫面請參考：

```
[root@modify-me ~]# x='() { :;}; echo vulnerable' bash -c "echo this is a test"
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
this is a test
[root@modify-me ~]#
```

檢測方法二：

1. 在 Shell 中輸入下列指令

```
env X='() { (shellshocker.net)=>\' bash -c "echo date"; cat echo ; rm -f echo
```

2. 依照系統回應資訊判斷是否需要更新

2.1. 若系統回應以下資訊，則表示**需要更新您的系統**

```
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
Tue Sep 30 16:42:47 CST 2014
```

實際畫面請參考：

```
[root@modify-me ~]# env X='() { (shellshocker.net)=>\' bash -c "echo date"; cat echo ; rm -f echo
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
Tue Sep 30 16:42:47 CST 2014
[root@modify-me ~]#
```

2.2. 若系統回應以下資訊，則表示**不需要更新您的系統**

```
date
```

實際畫面請參考：

```
[root@nagios ~]# env X='() { (shellshocker.net)=>\' bash -c "echo date"; cat echo ; rm -f echo
date
cat: echo: 沒有此一檔案或目錄
[root@nagios ~]#
```

修補方法

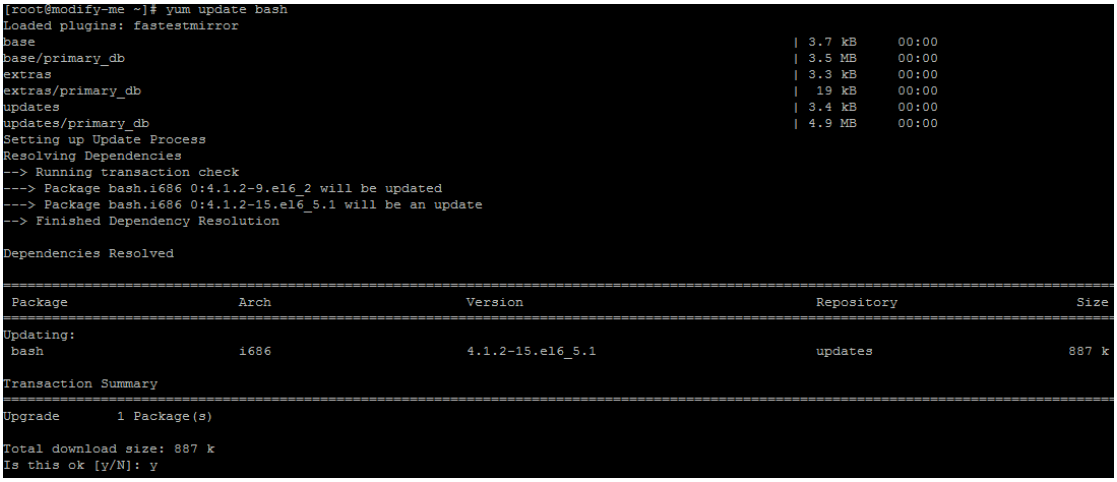
提供快速的修補步驟供使用者使用，請參閱修補方法一。若無法使用 yum 或是無法開通 80 port，則請參考修補方法二，直接下載檔案進行更新。

修補方法一：

1. 在 Shell 中輸入下列指令，使用 yum 下載並更新最新版的 Shell
   (注意：需使用 yum 及開通 80 port)

```
yum update bash
```

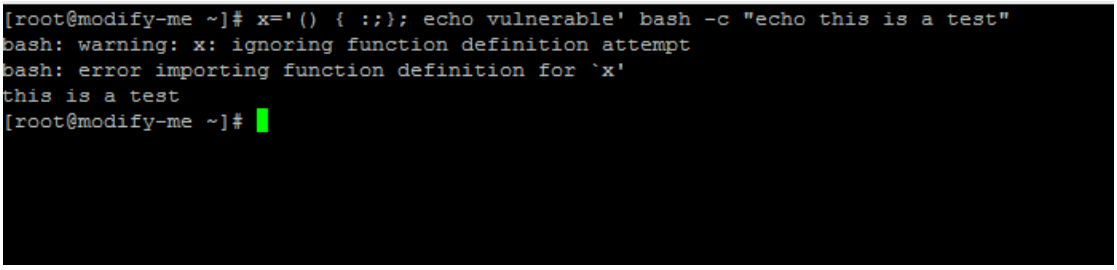
實際畫面請參考：



2. 更新完成後，請再次使用「檢測方法」檢驗您的系統，若系統回應以下資訊，則表示**<u>您的系統已經更新完成</u>**

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

實際畫面請參考：



修補方法二：

1. 請先利用以下指令確認版本及位元：
   (注意：主機無法使用 yum 或無法對外開通 80 port 時使用)

```
[root@mbtrial yum.repos.d]# cat /etc/issue
CentOS release 5.10 (Final)
Kernel \r on an \m
```

```
[root@mbtrial yum.repos.d]# uname –a
```

```
Linux mbtrial.openfind.com.tw 2.6.18-371.6.1.el5 #1 SMP Wed Mar 12
20:08:05 EDT 2014 i686 i686 i386 GNU/Linux
```

2. 針對不同版本，下載相對應的修復檔案：

CentOS 5	
i386	http://ftp.twaren.net/Linux/CentOS/5.10/updates/i386/RPMS/bash-3.2-33.el5_10.4.i386.rpm
x64	http://ftp.twaren.net/Linux/CentOS/5.10/updates/x86_64/RPMS/bash-3.2-33.el5_10.4.x86_64.rpm
CentOS 6	
i386	http://ftp.twaren.net/Linux/CentOS/6.5/updates/i386/Packages/bash-4.1.2-15.el6_5.2.i686.rpm
x64	http://ftp.twaren.net/Linux/CentOS/6.5/updates/x86_64/Packages/bash-4.1.2-15.el6_5.2.x86_64.rpm

3. 更新(需使用 root 權限安裝)：

```
su root
chmod +x xxx.rpm
rpm -Uvh xxx.rpm
```

網擎資訊軟體股份有限公司

地　　址：台北市 103 重慶北路二段 243 號 7 樓
電　　話：02-2553-2000　　傳　　真：02-2553-0707
網　　址：http://www.openfind.com
E-mail： m2k_noc@openfind.com