Replicant - Issue #1041

BASH (aka shellshock) vulnerability - CVE-2014-[6271/6277/6278/7169/7186/7187]

11/06/2014 10:20 AM - My Self

Status:	Closed	**Start date:**	11/06/2014
Priority:	High	**Due date:**	
Assignee:	Paul Kocialkowski	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	Any version	**Spent time:**	0.00 hour
Resolution:	fixed	**Grant:**	
Device:		**Type of work:**	

Description

I hope it's a good idea to open a bug ticket about the forum topic: http://redmine.replicant.us/boards/9/topics/6729

Summary
Replicant is (at the moment) vulnerable to the shellshock vulnerabilities.
Two patches "CVE-2014-6271 and CVE-2014-7169" are merged to Replicant in the meanwhile:
https://gitorious.org/replicant/external_bash/commits/64368c6fd95e4f749e6133398ad4d5fce3c9b940

But there are some more issues:
https://access.redhat.com/security/cve/CVE-2014-7186
https://access.redhat.com/security/cve/CVE-2014-7187
https://access.redhat.com/security/cve/CVE-2014-6277
https://access.redhat.com/security/cve/CVE-2014-6278
with available patches:
https://github.com/CyanogenMod/android_external_bash/commit/027626f9f273edf1c435c223f93768ec6dcc5301
https://github.com/CyanogenMod/android_external_bash/commit/bd2cb35e07e5cef774220e8b57bace207f162e50
https://github.com/CyanogenMod/android_external_bash/commit/369692c969182053c3a8f81775fa022934e3bd95
https://github.com/CyanogenMod/android_external_bash/commit/658bb3b21b2923f5e37dfe1ae2262fac5297d1af

Alternativly I would really appreciate it if the whole BASH version could be updated.
Here is the version "4.3.30" as a open source and shellshock fixed version, which I've successfully tested with Replicant 4.2:
https://github.com/3lo0sh/bash-arm

History

#1 - 11/08/2014 02:31 PM - Denis 'GNUtoo' Carikli

Hi,

There is an utility in f-droid to check for the vulnerability.
If you use it it'll tell that we're affected.

Do you know what do or can use bash in Replicant or f-droid?

I guess busybox or toolbox's shells are the ones that are used by default by almost everything.

Denis.

#2 - 11/08/2014 02:41 PM - Denis 'GNUtoo' Carikli

- Category changed from 51 to Security

#3 - 11/10/2014 11:34 AM - My Self

You mean this tool for sure: https://f-droid.org/repository/browse/?fdfilter=shellshock&fdid=in.indiandragon.shellshock.shellshockvulnerabilityscan
The problem with this tool is:
- that it checkes one single vulnerability (CVE-2014-6271) (http://blog.indiandragon.in/2014/10/shellshock-vulnerability-in-android.html) and
- after I manually (and temporarily) switched to the patched BASH over the CWM flashable zip file:
https://dl.dropboxusercontent.com/s/zbed1om7hgb5iqb/Bash-signed.zip?dl=0
Source: http://forum.xda-developers.com/android/software-hacking/dev-lastest-bash-android-t2898295
this tool still says, that I'm vulnerable with my new BASH version.

The last point is strange, because I've manually tested the Replicant built in BASH with that (CVE-2014-6271)-exploit over the Terminal Emulator app:
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"

which was vulnerable, and after the replacement to the patched BASH, I definitely verified, that I'm not vulnerable to this exploit anymore, (with exactly the same test of course)...
Source & exploits for the other CVEs: https://shellshocker.net/

#4 - 11/16/2014 10:37 AM - Paul Kocialkowski

The commits from CyanogenMod cannot be fetched (even though they show up on the github website), please provide commits I can include directly in Replicant.

I don't like the idea of updating components versions, it makes things hard to maintain, so I prefer to backport patches (i.e. I want updates to be only security-related, not features-related). If there is no other way, I will consider bumping the version, but please try to find a way for me to integrate those patches in the current code.

#5 - 11/16/2014 10:43 AM - Paul Kocialkowski

Nevermind, I found a way to export the patches:
https://github.com/CyanogenMod/android_external_bash/commit/027626f9f273edf1c435c223f93768ec6dcc5301.patch

#6 - 11/28/2014 09:22 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Everything pushed to the repositories, will be part of the next batch of images.

#7 - 12/01/2014 11:15 AM - Paul Kocialkowski

Note that the applications still says that it is vulnerable, but it may just be checking the bash version, which didn't change since I just backported the patches.

I tried with the script from: https://shellshocker.net/

Results on the 0002 images:

```
CVE-2014-6271 (original shellshock): VULNERABLE
CVE-2014-6277 (segfault): not vulnerable
CVE-2014-6278 (Florian's patch): VULNERABLE
bash: line 39: cd: /tmp: No such file or directory
CVE-2014-7169 (taviso bug): VULNERABLE
bash: line 50:  4872 Segmentation fault      bash -c 'true <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<EOF <<E
OF <<EOF <<EOF <<EOF <<EOF <<EOF' 2> /dev/null
CVE-2014-7186 (redir_stack bug): VULNERABLE
CVE-2014-7187 (nested loops off by one): not vulnerable
CVE-2014-//// (exploit 3 on http://shellshocker.net/): not vulnerable
```

Results with the current repositories:

```
CVE-2014-6271 (original shellshock): not vulnerable
CVE-2014-6277 (segfault): not vulnerable
CVE-2014-6278 (Florian's patch): not vulnerable
bash: line 39: cd: /tmp: No such file or directory
CVE-2014-7169 (taviso bug): not vulnerable
CVE-2014-7186 (redir_stack bug): not vulnerable
CVE-2014-7187 (nested loops off by one): not vulnerable
CVE-2014-//// (exploit 3 on http://shellshocker.net/): not vulnerable
```