

This repository has been archived by the owner. It is now read-only.

hyn9 / VIKIROOT Archived

CVE-2016-5195 (Dirty COW) PoC for Android 6.0.1 Marshmallow

GPL-3.0 License

253 stars 107 forks

Star

Watch

Code

Issues 5

Pull requests

Actions

Projects

Wiki

Security

master

...



hyn9 dump before check kernel ...

on Jan 27, 2017

20

[View code](#)

README.md

VIKIROOT

This is a CVE-2016-5195 PoC for 64-bit Android 6.0.1 Marshmallow (perhaps 7.0 ?), as well as an universal & stable temporal root tool. It does not require a SUID executable or any filesystem changes.

Features

- SELinux bypass (see below for details).
- Memory-only: does not modify the filesystem or need special executable.
- Stable: does not affect stability of your device.
- Scalable: easy to add new kernel and/or new devices.
- Reversible: the backdoor is cleared automatically after the root shell ends, which means no reboot is required after usage.

Attention

By "SELinux bypass" I mean the payload will run in init domain even if SELinux is in enforcing mode, however, a patch to sepolicy is still needed for making init domain unconfined. Usually this means a modified boot image is required.

Prerequisite

- *I, Robot* by Isaac Asimov.
- "dirtycow-capable" device.
- patched sepolicy.

Building

Pre-built binaries are available on the release page. Otherwise, just add NDK standalone toolchain into `PATH` and run `make`.

Usage

You may run it through an adb shell (place it under `/data/local/tmp`) and get a root shell either in the built-in terminal or a remote terminal server such as nc. For details, run it without any parameters.

Troubleshooting

- firstly please read through the "Attention" part above.
- "insufficient place for payload" or "unknown kernel": a reboot is required.
- "waiting for reverse connect shell": please wake up your device, open the clock/alarm app or toggle the bluetooth switch in order to trigger the backdoor.
- still no luck: please run the "dbg" version and send an e-mail to me with the generated files which are just dump of some part of kernel and don't contain any personal information.

Credits

- scumjr for the vDSO patching method.
- Tzul for helping me debug the sepolicy problem.
- RenaKunisaki for making it work with bionic.

TODO

- Enrich the kernel database for x86 support and so on.
- Test it on Android 7 Nougat (help wanted!).

Releases

 2 tags

Packages

No packages published

Languages

● C 76.5% ● Assembly 21.3% ● Makefile 2.2%