Published on *Tux Machines* (http://www.tuxmachines.org)

Security: Patches, Roboto Drama and Android/Google

By *Roy Schestowitz*
Created *22/11/2019 - 6:37pm*
Submitted by Roy Schestowitz on Friday 22nd of November 2019 06:37:38 PM Filed under Security [1]

- **Security updates for Friday [2]**

  > Security updates have been issued by Fedora (dpdk, mingw-djvulibre, mingw-hunspell, mingw-ilmbase, mingw-OpenEXR, php-symfony, php-symfony3, and rsyslog), openSUSE (chromium and squid), SUSE (aspell, cups, djvulibre, and dpdk), and Ubuntu (djvulibre).

- **Roboto Botnet network building, DDoS not a priority [3]**

- **Google quintuples top reward for hacking Android to $1 million [4]**

  > Google, which has already paid security researchers over $15 million since launching its bug bounty program in 2010, today expanded its Android Security Rewards program. Most notably, the company is introducing a top prize of $1 million. The previous top prize was $200,000. That?s technically a quintupling, although the maximum reward could be even higher. Google is launching a 50% bonus for exploits found on specific developer preview versions of Android, meaning the top reward could net you $1.5 million.

- **Bad Binder: Android In-The-Wild Exploit (Project Zero) [5]**

  > Over on the Project Zero blog, Maddie Stone has a lengthy post about a zero-day exploit that was found and fixed in the Android Binder interprocess communication mechanism. The post

details the search for the problem, which was apparently being used in the wild, its fix, and how it can be exploited. This is all part of an effort to "make zero-day hard"; one of the steps the project is taking is to disseminate more information on these bugs.

- **Bad Binder: Android In-The-Wild Exploit [6]**

  On October 3, 2019, we disclosed issue 1942 (CVE-2019-2215), which is a use-after-free in Binder in the Android kernel. The bug is a local privilege escalation vulnerability that allows for a full compromise of a vulnerable device. If chained with a browser renderer exploit, this bug could fully compromise a device through a malicious website.

  We reported this bug under a 7-day disclosure deadline rather than the normal 90-day disclosure deadline. We made this decision based on credible evidence that an exploit for this vulnerability exists in the wild and that it's highly likely that the exploit was being actively used against users.

  In May 2019, Project Zero published a blog post and spreadsheet for tracking ?in-the-wild? 0-day exploits. In July 2019, I joined Project Zero to focus on the use of 0-day exploits in the wild. We expect our approach to this work will change and mature as we gain more experience with studying 0-days, but the mission stays the same: to ?make zero-day hard?.

Security

Source URL: http://www.tuxmachines.org/node/130816

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/805367/rss
[3] https://www.scmagazineuk.com/roboto-botnet-network-building-ddos-not-priority/article/1666590
[4] https://venturebeat.com/2019/11/21/google-quintuples-top-reward-for-hacking-android-to-1-million/
[5] https://lwn.net/Articles/805321/rss
[6] https://googleprojectzero.blogspot.com/2019/11/bad-binder-android-in-wild-exploit.html