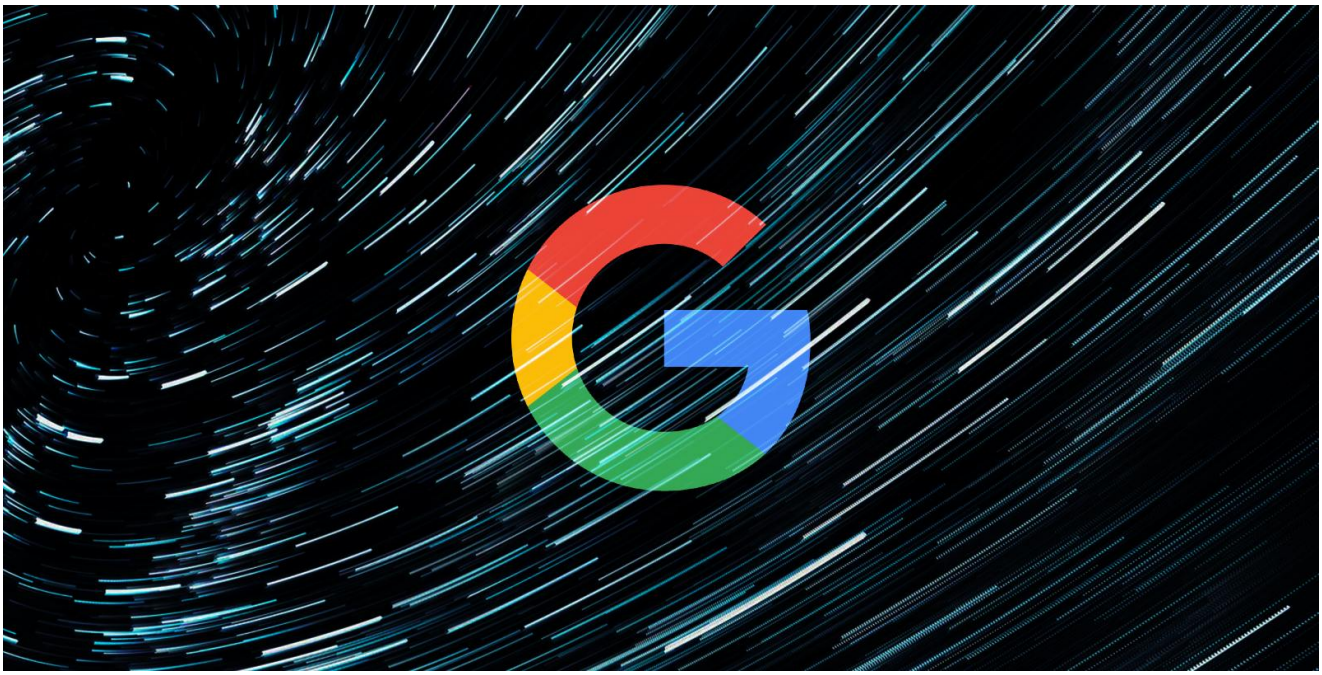
May Android security updates patch 4 zero-days exploited in the wild

bleepingcomputer.com/news/security/may-android-security-updates-patch-4-zero-days-exploited-in-the-wild/

Sergiu Gatlan

By
Sergiu Gatlan

- May 19, 2021
- 12:53 PM
- 0



According to info provided by Google's Project Zero team, four Android security vulnerabilities were exploited in the wild as zero-day bugs before being patched earlier this month.

Attacks attempting to exploit these flaws were targeted and impacted a limited number of users based on information shared after this month's Android security updates were published.

"There are indications that CVE-2021-1905, CVE-2021-1906, CVE-2021-28663 and CVE-2021-28664 may be under limited, targeted exploitation," a recently updated version of the May 2021 Android Security Bulletin reveals.

> For 2021, we've surpassed the number of 0-days detected in-the-wild in all of 2020. That's great!https://t.co/o4F74b68Fh
>
> — Maddie Stone (@maddiestone) May 19, 2021

The four Android vulnerabilities impact Qualcomm GPU and Arm Mali GPU Driver components.

Qualcomm and Arm have published further details on each vulnerability via security advisories issued separately [1, 2].

Android users are recommended to install this month's security updates as soon as possible if they are impacted by these issues.

CVE-ID	Impact
CVE-2021-1905	Qualcomm - Use After Free in Graphics. Possible use after free due to improper handling of memory mapping of multiple processes simultaneously.
CVE-2021-1906	Qualcomm - Detection of Error Condition Without Action in Graphics. Improper handling of address deregistration on failure can lead to new GPU address allocation failure.
CVE-2021-28663	ARM - Mali GPU Kernel Driver allows improper operations on GPU memory. A non-privileged user can make improper operations on GPU memory to enter into a use-after-free scenario and may be able to gain root privilege, and/or disclose information.
CVE-2021-28664	ARM - Mali GPU Kernel Driver elevates CPU RO pages to writable. A non-privileged user can get a write access to read-only memory, and may be able to gain root privilege, corrupt memory and modify the memory of other processes.

This month's Android security updates also include patches for critical vulnerabilities in the System component that could be exploited by remote attackers using specially crafted files to execute arbitrary malicious code within the context of a privileged process.

Regrettably, users who haven't switched to new devices that still receive monthly security updates might not be able to install these patches.

To put things into perspective, more than 9% of all Android devices are still running Android 8.1 Oreo (released in December 2017), and roughly 19% Android Pie 9.0 (released in August 2018), according to StatCounter data.

In December, Qualcomm also addressed a high severity security vulnerability in Mobile Station Modem (MSM) chips (including the latest 5G-capable versions) that could allow attackers to access smartphone users' text messages, call history, and listen in on their conversations.

Last year, Qualcomm fixed more vulnerabilities impacting the Snapdragon chip Digital Signal Processor (DSP) chip and enabling attackers to take control of smartphones without user interaction and create unremovable malware that can evade detection.

Other bugs that could allow decrypting some WPA2-encrypted wireless network packets, accessing critical data, and two flaws in the Snapdragon SoC WLAN firmware allowing over the air compromise of the modem and the Android kernel were also patched during the last two years.

Related Articles:

Google: Predator spyware infected Android devices using zero-days

Google Chrome emergency update fixes zero-day used in attacks

Microsoft finds severe bugs in Android apps from large mobile providers

Mozilla fixes Firefox, Thunderbird zero-days exploited at Pwn2Own

CISA adds 41 vulnerabilities to list of bugs used in cyberattacks