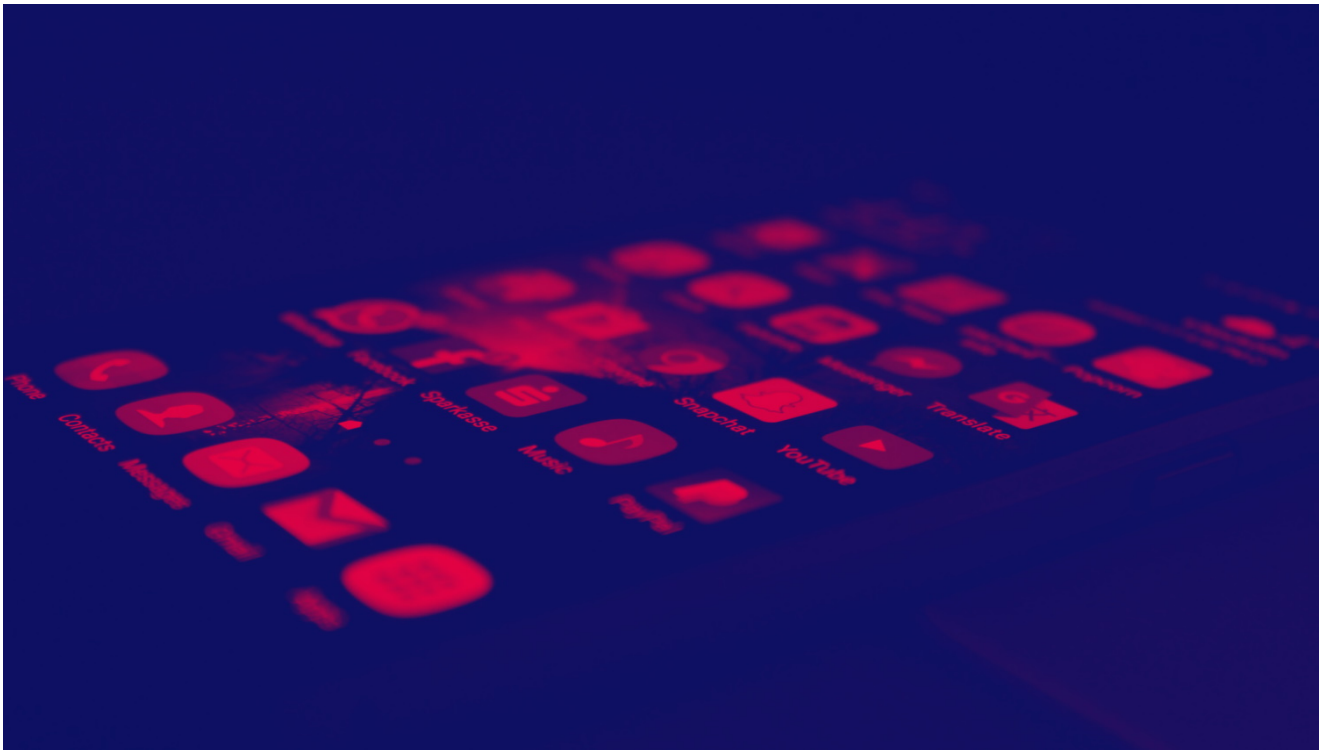
Google fixes Android zero-day exploited in the wild in targeted attacks

therecord.media/google-fixes-android-zero-day-exploited-in-the-wild-in-targeted-attacks/

November 4, 2021



Google has released on Monday its monthly Android security bulletin, and the company's engineers said they patched a zero-day vulnerability that was being exploited in the wild in what they described as "limited, targeted exploitation."

Tracked as **CVE-2021-1048**, Google said the vulnerability resided in one of the Android kernel components and was abused to elevate an attacker's privileges.

Details about the attacks, the threat actor(s) behind them, and the victims have not been shared, as is the standard practice for most security patches. This approach is used in order to give end-users more time to update their vulnerable devices before the same bug is weaponized by other threat actors.

CVE-2021-1048 marks the sixth Android zero-day vulnerability that was exploited this year.

Google patched similar zero-days in the January and May Android security bulletins as well.

The previous zero-days didn't impact the Android OS kernel itself but rather add-on components from Qualcomm and Arm, respectively.

- **CVE-2021-11261** – Memory management logic error in Qualcomm kgsl graphics driver.

- **CVE-2021-1905** – Use-after-free vulnerability in Qualcomm GPU.
- **CVE-2021-1906** – Improper error handling in Qualcomm GPU.
- **CVE-2021-28663** – Use-after-free vulnerability in Arm's Mali GPU.
- **CVE-2021-28664** – Writes to read-only memory bug in Arm's Mali GPU.

While six vulnerabilities were exploited in Android devices before patches were available (hence the zero-day categorization), Apple has had a harder time this year and the company patched 15 zero-days this year that impacted its iOS/iPhone userbase.

Tags

- Android
- Android security bulletin
- Google
- security update
- vulnerability disclosure
- zero-day

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.