



Exynos Modems



Overview

Google Project Zero [listed 18 vulnerabilities](#) in Samsung Exynos modems produced by Samsung Semiconductor. The four most severe vulnerabilities are CVE-2023-24033, CVE-2023-26496, CVE-2023-26497 and CVE-2023-26498, which allow for remote exploitation of the baseband from the internet, thereby permitting attackers to compromise the phone without any user interaction. It only requires the attacker to know the victim's phone number. The other 14 vulnerabilities are not as severe as they either need a malicious mobile network operator or local access to the device. Affected device models:

- Devices from Samsung, including those in the S22, M33, M13, M12, A71, A53, A33, A21s, A13, A12 and A04 series;
- Mobile devices from Vivo, including those in the S16, S15, S6, X70, X60 and X30 series;
- The Pixel 6 and Pixel 7 series of devices from Google

While the affected Pixel devices have received fixes for all four CVEs mentioned above in their March ASPL update, others have not yet released a patch. In the case of a compromised device, Lookout will be able to detect the compromise and alert both the user and the admin. Users with affected devices, if allowed by the carrier, can also protect themselves by turning off WiFi calling and voice over LTE in their device settings.

Lookout Coverage and Recommendation for Admins

Lookout provides multilayered protection for devices that are exploitable through multiple vectors. We strongly suggest users keep their devices on auto update for security fixes as they become available. Lookout will detect if an attacker is successfully able to compromise the device at the OS level.

Lookout admins should configure policies to the appropriate risk/response level. They can then choose whether to alert the user that the device is out of compliance or block access to enterprise resources.

Lookout Analysis

While there has only been a limited amount of information published regarding these vulnerabilities, we know that CVE-2023-24033, CVE-2023-26496, CVE-2023-26497 and CVE-2023-26498 are capable of remote code execution and should be considered highly severe. An attacker would likely use these vulnerabilities as an entry point to a device and then pivot from the baseband to compromise the operating system running on the application processor where they would have access to user data.

Lookout Vulnerability and Patch Management

Lookout Vulnerability and Patch Management enables you to know every version of an operating system and mobile app in your organization. We provide visibility into device risk whether it is company- or employee-owned, as well as managed or unmanaged.

[Click here to learn more about Vulnerability & Patch Management](#)