



CVE-2021-25337/369/370



Overview

Google's Threat Analysis Group (TAG) under Project Zero recently revealed an active kill chain that exploits vulnerabilities in Samsung devices. The affected devices are built with the Exynos SOC chip, which is one of the most common chips used in Samsung devices and run kernel version 4.14.113. These exploits are believed to belong to a commercial surveillance vendor and the three vulnerabilities they take advantage of are detailed below. They can all be patched by the March 2021 Samsung security patch.

Coverage and Recommendation for Lookout Admins

Lookout admins should proactively enable the vulnerability protection policy in the Lookout console. Using the out-of-date Android Security Patch Level at March 2021 or higher and risk level for vulnerable applications will help avoid this kill chain. As of November 17th, 2022, Lookout will alert versions prior to 3.0.05.7 of Samsung Text-to-Speech as vulnerable. The coverage can be tracked as Samsung-CVE-2021-25337.gen. In addition, CISA is requiring all government organizations to update these apps by November 29th.

Lookout Analysis

Together, the three vulnerabilities form a kill chain. For initial access, the Samsung clipboard runs as the system user and leverages CVE-2021-25337 to grant arbitrary file read and write capabilities. It then provides privileged access at the Android OS level via the system server and reuses the same CVE to execute code via the Samsung Text-to-Speech app. From here, the kill chain utilizes CVE-2021-25369 for an information leak of the kernel address via `sec_log`. The third vulnerability, CVE-2021-25370, lies in the display and enhancement controller that creates video signals, and is used to gain arbitrary kernel read and write access using the DPU driver.

The most likely way for an attacker to exploit this vulnerability would be to gain initial access onto the device through a malicious application that can access the clipboard. The following MITRE techniques could be in play: Command and Scripting Interpreter [T1623](#), Abuse Elevation Control Mechanism [T1626](#), Native API (Execution, [T1575](#)), and Software Discovery [T1418](#). The Samsung Text-to-Speech application can be updated via the Samsung Galaxy store, not the Google Play Store.

Lookout Mobile Vulnerability and Patch Management

Lookout Mobile Vulnerability and Patch Management enables you to know every operating system and mobile app version in your fleet. We provide visibility into device risk whether it is company- or employee-owned, managed, or unmanaged. Lookout crowdsources the most comprehensive vulnerability and patch management database from analysis of over 210 million mobile devices and 175 million apps. It correlates the app and operating system versions needed to patch vulnerabilities. In addition, the database specifies the version of the operating system that is specific to a carrier and device manufacturer for the patch.

[Click here to learn more about Lookout Mobile Vulnerability and Patch Management](#)