Preinstalled Android Apps on Samsung Devices

Overview

It was recently discovered that a handful of preinstalled Android apps had vulnerabilities that could be exploited on exposed Samsung devices. The initial analysis of these apps by Oversecured shows that the vulnerabilities could allow threat actors to access and edit the victim's contacts, calls, SMS and MMS, install arbitrary apps with device administrator rights, or read and write files on behalf of a user to change the device's settings. Below is a list of the affected apps and descriptions of the potential malicious actions:

- Knox Core (CVE-2021-25388): Attackers can install arbitrary apps on the device.
- Managed Provisioning (CVE-2021-25356): Attackers can install third-party apps and grant device admin privileges.
- Secure Folder (CVE-2021-25391): Attackers can execute privileged actions.
- SecSettings (CVE-2021-25393): Attackers can get permission to access system UID data.
- Samsung DeX System UI (CVE-2021-25392): Attackers can exfiltrate sensitive information by changing the backup path configuration.
- TelephonyUI (CVE-2021-25397): Attackers can write arbitrary files of telephony processes via untrusted apps.
- PhotoTable (CVE-2021-20724): Attackers can execute privileged actions.

Recommendation for Lookout Admins

Any device with Android Security Patch Level (ASPL) later that 2021-05-05 will be protected from exploitation of these vulnerabilities. With that in mind, Lookout Admins should set the minimum required ASPL as 2021-05-05 if the user wants to access any corporate resources from their mobile device. By implementing access policies that only allow users and devices with the most up-to-date app versions installed on their devices, Lookout admins can ensure that threat actors don't use vulnerable apps to access sensitive data.

Lookout Analysis

Access to these types of data could lead to corporate data leakage and compliance violations if the device user has stored sensitive files locally on their device or communicated with colleagues about sensitive topics like research and development projects. Attackers know that mobile devices can access corporate data but oftentimes aren't secured in the same way as laptops and desktops with access to the same data. To exploit these vulnerabilities, an attacker would most likely build a malicious third-party app that they would convince targeted victims to download through socially engineered mobile phishing campaigns.

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