BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

November 8, 2023

Multiple Vulnerabilities in Google Android OS Could Allow for Privilege Escalation

OVERVIEW

Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for privilege escalation. Android is an operating system developed by Google for mobile devices, including, but not limited to, smartphones, tablets, and watches. Successful exploitation of the most severe of these vulnerabilities could allow for privilege escalation. Depending on the privileges associated with the exploited component, an attacker could then install programs; view, change, or delete data; or create new accounts with full rights.

THREAT INTELLIGENCE

- There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED

- Android OS patch levels prior to 2023-11-05

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY

Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for privilege escalation in the context of the affected component. Following the MITRE ATT&CK framework, exploitation of these vulnerabilities can be classified as follows:

Tactic: Privilege Escalation (TA0004):

Technique: Exploitation for Privilege Escalation (T1068):

- Multiple vulnerabilities in Framework that could allow for escalation of privilege. (CVE-2023-40106, CVE-2023-40107, CVE-2023-40109, CVE-2023-40110, CVE-2023-40111, CVE-2023-40114)
- Multiple vulnerabilities in System that could allow for escalation of privilege. (CVE-2023-40100, CVE-2023-40115)

Details of lower-severity vulnerabilities are as follows:

- A vulnerability in System that could allow for information disclosure. (CVE-2023-40113)
- Multiple vulnerabilities in Framework that could allow for information disclosure. (CVE-2023-40105, CVE-2023-40124)

- Multiple vulnerabilities in System that could allow for information disclosure. (CVE-2023-40104, CVE-2023-40112)
- Multiple vulnerabilities in System that could allow for denial of service. (CVE-2023-21103, CVE-2023-21111)
- Multiple vulnerabilities in Project Mainline components. (CVE-2023-40100, CVE-2023-40115)
- A vulnerability in Arm components. (CVE-2023-28469)
- A vulnerability in MediaTek components. (CVE-2023-32832, CVE-2023-32834, CVE-2023-32835, CVE-2023-32836, CVE-2023-32837, CVE-2023-20702)
- Multiple vulnerabilities in Qualcomm components. (CVE-2023-33031, CVE-2023-33055, CVE-2023-33059, CVE-2023-33074)
- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2023-21671, CVE-2023-22388, CVE-2023-28574, CVE-2023-33045, CVE-2023-24852, CVE-2023-28545, CVE-2023-28556, CVE-2023-33047, CVE-2023-33048, CVE-2023-33056, CVE-2023-33061)

Successful exploitation of the most severe of these vulnerabilities could allow for privilege escalation. Depending on the privileges associated with the exploited component, an attacker could then install programs; view, change, or delete data; or create new accounts with full rights.

RECOMMENDATIONS

We recommend the following actions be taken:

- Apply appropriate updates and patches provided by Google to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
  - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
  - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
  - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
  - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
- Restrict execution of code to a virtual environment on or in transit to an endpoint system. **(M1048: Application Isolation and Sandboxing)**
  - **Safeguard 16.8: Separate Production and Non-Production Systems:** Maintain separate environments for production and non-production systems.

REFERENCES
Google:

- https://source.android.com/docs/security/bulletin/2023-11-01#2023-11-05-security-patch-level-vulnerability-details

CVE:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20702
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21103
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21111
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21671
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22388
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24852
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28469
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28545
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28556
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28574
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32832
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32834
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32835
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32836
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32837
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33031
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33045
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33047
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33048
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33055
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33056
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33059
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33061
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33074
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40100
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40100
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40104
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40105
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40106
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40107
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40109
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40110
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40111
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40112
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40113
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40114
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40115
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40115
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40124