TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
10/04/2022

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for arbitrary code execution. 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 arbitrary code execution. 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 2022-10-01

RISK:
Government:

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

Businesses:

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

Home users: Low

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

Tactic: *Execution* (TA0002):

    Technique: *Exploitation for Client Execution* (T1203):

- Multiple vulnerabilities in Qualcomm closed-source components that could lead to arbitrary code execution. (CVE-2022-25718, CVE-2022-25748)

Details of lower-severity vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could allow for escalation of privilege. (CVE-2022-20420, CVE-2021-39758, CVE-2022-20415)
- Multiple vulnerabilities in Framework that could allow for information disclosure. (CVE-2022-20419, CVE-2022-20351)
- Multiple vulnerabilities in Framework that could allow for Denial of Service. (CVE-2021-39624)
- Multiple vulnerabilities in Media Framework that could allow for information disclosure. (CVE-2022-20413, CVE-2022-20418)
- Multiple vulnerabilities in System that could allow for escalation of privilege. (CVE-2022-20412, CVE-2022-20416, CVE-2022-20417)
- Multiple vulnerabilities in System that could allow for information disclosure. (CVE-2021-39673, CVE-2022-20394, CVE-2022-20410)
- Multiple vulnerabilities in System that could allow for Denial of Service. (CVE-2022-20425)
- Multiple vulnerabilities in Kernel that could allow for escalation of privilege. (CVE-2022-20421, CVE-2022-20422, CVE-2022-20423, CVE-2022-20424)
- Multiple vulnerabilities in Kernel components that could allow for escalation of privilege. (CVE-2022-20409)
- Multiple vulnerabilities in Imagination Technologies components. (CVE-2021-0696, CVE-2021-0951, CVE-2021-0699)
- Multiple vulnerabilities in Unisoc components. (CVE-2022-20430, CVE-2022-20431, CVE-2022-20432, CVE-2022-20433, CVE-2022-20434, CVE-2022-20435, CVE-2022-20436, CVE-2022-20437, CVE-2022-20438, CVE-2022-20439, CVE-2022-20440)
- Multiple vulnerabilities in Qualcomm components. (CVE-2022-25720, CVE-2022-22077, CVE-2022-25723, CVE-2022-33214, CVE-2022-33217)
- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2022-25660, CVE-2022-25661, CVE-2022-25687, CVE-2022-25736, CVE-2022-25749)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. 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 patches provided by Google to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
    - o **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.
    - o **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.
    - o **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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources. (**M1017: User Training**)
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection)**
    - o **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Apple® System Integrity Protection (SIP) and Gatekeeper™.

REFERENCES:

Google:
https://source.android.com/docs/security/bulletin/2022-10-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0651
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0699
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39673
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20351
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20394
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20409
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20410
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20412
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20413
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20416

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20417
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20418
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20419
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20420
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20421
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20422
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20423
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20424
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20430
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20431
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20432
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20435
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20436
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20438
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20440
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22077
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25660
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25687
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25718
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25723
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25736
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33214
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33217