TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
07/08/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (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 within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
  • Android OS builds utilizing Security Patch Levels issued prior to July 5, 2021.

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 within the context of a privileged process. Details of these vulnerabilities are as follows:
  • A vulnerability in Media Framework that could allow for Escalation of Privilege (CVE-2021-0587)

- A vulnerability in Media Framework that could allow for Information Disclosure (CVE-2021-0601)
- A vulnerability in Framework that could allow for Escalation of Privileges (CVE-2021-0441, CVE-2021-0486)
- A vulnerability in Framework that could allow for Information Disclosure (CVE-2020-0368)
- Multiple vulnerabilities in System that could allow for Escalation of Privileges (CVE-2020-0417, CVE-2021-0585, CVE-2021-0586, CVE-2021-0589, CVE-2021-0594, CVE-2021-0600, CVE-2021-0602, CVE-2021-0603)
- Multiple vulnerabilities in System that could allow for Information Disclosure (CVE-2021-0518, CVE-2021-0588, CVE-2021-0590, CVE-2021-0596, CVE-2021-0597, CVE-2021-0599, CVE-2021-0604)
- A high severity vulnerability in MediaTek components (CVE-2021-0577)
- A critical severity in Widevine DRM (CVE-2021-0592)
- A critical severity vulnerability in Qualcomm components (CVE-2021-1965)
- Multiple high severity vulnerability in Qualcomm components (CVE-2021-1907, CVE-2021-1931, CVE-2021-1940, CVE-2021-1943, CVE-2021-1945, CVE-2021-1954, CVE-2021-1955, CVE-2021-1964, CVE-2021-1970)
- Multiple critical and high severity vulnerabilities in Qualcomm closed-source components (CVE-2020-11307, CVE-2021-1886, CVE-2021-1888, CVE-2021-1889, CVE-2021-1890, CVE-2021-1938, CVE-2021-1953)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution within the context of a privileged process. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate updates by Google Android or mobile carriers to vulnerable systems, immediately after appropriate testing.
- Remind users to only download applications from trusted vendors in the Play Store.
- 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.

REFERENCES:
Google Android:
https://source.android.com/security/bulletin/2021-07-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0368
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0417
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11307
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0441
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0486
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0515

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0577
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0585
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0589
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0590
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0592
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0594
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0596
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0597
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0599
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0600
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0601
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0602
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0603
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0604
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1886
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1888
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1907
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1938
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1940
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1945
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1954
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1970