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:
05/04/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for remote 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 remote 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 May 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 remote code execution within the context of a privileged process. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could allow for Escalation of Privileges (CVE-2021-0472, CVE-2021-0485, CVE-2021-0487, CVE-2019-2219)
- A vulnerability in Media Framework that could allow for Escalation of Privilege (CVE-2021-0482)
- A vulnerability in Media Framework that could allow for Information Disclosure (CVE-2021-0484)
- Multiple vulnerabilities in System that could allow for Remote Code Execution (CVE-2021-0473, CVE-2021-0474, CVE-2021-0475)
- Multiple vulnerabilities in System that could allow for Escalation of Privilege (CVE-2021-0476, CVE-2021-0477, CVE-2021-0481)
- Multiple vulnerabilities in System that could allow for Information Disclosure (CVE-2021-0466, CVE-2021-0480)
- A vulnerability in Kernel Components that could allow for Escalation of Privilege (CVE-2020-29661)
- A Critical severity vulnerability in AMLogic components (CVE-2021-0467)
- Multiple High severity vulnerabilities in ARM components (CVE-2021-28663, CVE-2021-28664)
- Multiple High severity vulnerabilities in MediaTek components (CVE-2021-0489, CVE-2021-0490, CVE-2021-0491, CVE-2021-0492, CVE-2021-0493, CVE-2021-0494, CVE-2021-0495, CVE-2021-0496, CVE-2021-0497, CVE-2021-0498)
- A High severity vulnerability in Unisoc components (CVE-2021-0324)
- Multiple High severity vulnerabilities in Qualcomm components (CVE-2021-1891, CVE-2021-1905, CVE-2021-1927)
- A Moderate severity vulnerability in Qualcomm components (CVE-2021-1906)
- Multiple High severity vulnerabilities in Qualcomm closed-source components (CVE-2020-11273, CVE-2020-11274, CVE-2020-11279, CVE-2020-11284, CVE-2020-11285, CVE-2020-11288, CVE-2020-11289, CVE-2021-1910, CVE-2021-1915)

Successful exploitation of the most severe of these vulnerabilities could allow for remote 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/2021-05-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2219

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11273
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11274
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11279
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11284
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11285
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11288
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11289
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0324
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0466
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0467
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0475
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0477
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0481
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0482
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0484
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0485
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0487
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0491
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0493
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0494
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0495
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0496
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0497
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0498
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1905
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1915
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28663
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28664