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:
06/08/2021

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 June 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:

- A vulnerability in Android runtime that could allow for Escalation of Privileges (CVE-2021-0511)
- A vulnerability in Framework that could allow for Information Disclosure (CVE-2021-0521)
- A vulnerability in Framework that could allow for Escalation of Privileges (CVE-2021-0513)
- Multiple vulnerabilities in Media Framework that could allow for Escalation of Privileges (CVE-2021-0508, CVE-2021-0509, CVE-2021-0510, CVE-2021-0520)
- A vulnerability in System that could allow for Remote Code Execution (CVE-2021-0507)
- Multiple vulnerabilities in System that could allow for Escalation of Privileges (CVE-2021-0516, CVE-2021-0505, CVE-2021-0506, CVE-2021-0523, CVE-2020-26555, CVE-2020-26558, CVE-2021-0478)
- Multiple vulnerabilities in System that could allow for Information Disclosure (CVE-2021-0504, CVE-2021-0517, CVE-2021-0522)
- Multiple vulnerabilities in Kernel components that could allow for Escalation of Privileges (CVE-2020-143055, CVE-2021-0512)
- Multiple high severity vulnerabilities in MediaTek components (CVE-2021-0525, CVE-2021-0526, CVE-2021-0527, CVE-2021-0528, CVE-2021-0529, CVE-2021-0530, CVE-2021-0531, CVE-2021-0532, CVE-2021-0533)
- A high severity vulnerability in Qualcomm components (CVE-2020-11267)
- Multiple critical and high severity vulnerabilities in Qualcomm closed-source components (CVE-2020-11176, CVE-2020-11291, CVE-2020-26558, CVE-2020-11292, CVE-2020-11298, CVE-2020-11304, CVE-2020-11306, CVE-2020-26555, CVE-2021-1900, CVE-2021-1925, CVE-2021-1937)

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/2021-06-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11176
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11267
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11298
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11304

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11306
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26558
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0478
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0504
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0505
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0506
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0507
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0508
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0511
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0517
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0520
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0522
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0523
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0525
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0527
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0529
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0530
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0532
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1925
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1937