TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
01/04/2021

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 January 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: High

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-2021-0303, CVE-2021-0306, CVE-2021-0307, CVE-2021-0310, CVE-2021-0315, CVE-2021-0317, CVE-2021-0318, CVE-2021-0319)
- A vulnerability in Framework that could allow for Remote Code Execution (CVE-2020-15999)
- Multiple vulnerabilities in Framework that could allow for Information Disclosure (CVE-2021-0304, CVE-2021-0309, CVE-2021-0321, CVE-2021-0322)
- Multiple vulnerabilities in Framework that could allow for Denial of Service (CVE-2021-0313, CVE-2019-9376)
- A vulnerability in Media Framework that could allow for Remote Code Execution (CVE-2016-6328)
- Multiple vulnerabilities in Media Framework that could allow for Information Disclosure (CVE-2021-0311, CVE-2021-0312)
- Multiple vulnerabilities in System that could allow for Escalation of Privileges (CVE-2020-0471, CVE-2021-0308)
- A vulnerability in System that could allow for Remote Code Execution (CVE-2021-0316)
- A vulnerability in System that could allow for Information Disclosure (CVE-2021-0320)
- Multiple vulnerabilities in Kernel components that could allow for Information Disclosure (CVE-2020-10732, CVE-2020-10766, CVE-2021-0323)
- A high severity vulnerability in MediaTek components (CVE-2021-0301)
- Multiple high severity vulnerabilities in Qualcomm components (CVE-2020-11233, CVE-2020-11239, CVE-2020-11240, CVE-2020-11250, CVE-2020-11261, CVE-2020-11262)
- Multiple critical severity vulnerabilities in Qualcomm closed-source components (CVE-2020-11134, CVE-2020-11182)
- Multiple high severity vulnerabilities in Qualcomm closed-source components (CVE-2020-11126, CVE-2020-11159, CVE-2020-11181, CVE-2020-11235, CVE-2020-11238, CVE-2020-11241, CVE-2020-11260)

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/2021-01-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6328
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9376
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0471
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10732
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11126
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11134
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11159
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11233
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11235
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11238
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11239
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11240
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11241
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11250
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11260
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11261
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11262
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0301
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0303
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0304
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0306
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0307
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0308
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0309
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0310
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0311
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0312
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0313
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0315
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0316
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0317
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0318
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0319
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0320
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0321
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0322
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0323