The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

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

DATE(S) ISSUED:
05/03/2022

SUBJECT:
Multiple Vulnerabilities in Google Android OS Could Allow for Escalation of Privilege

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (OS), the most severe of which could allow for escalation of privilege. 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 escalation of privilege. 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, 2022

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 escalation of privilege. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities in Framework, the most severe vulnerability in this section could lead to local escalation of privilege with User execution privileges needed.(CVE-2021-39662, CVE-2022-20004, CVE-2022-20005, CVE-2022-20007, CVE-2021-39700)
- Multiple vulnerabilities in System, the most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed.(CVE-2022-20113, CVE-2022-20114, CVE-2022-20116, CVE-2022-20010, CVE-2022-20011, CVE-2022-20115, CVE-2021-39670, CVE-2022-20112)
- A vulnerability in the MediaProvider component of Project Mainline (CVE-2021-39662)
- Multiple vulnerabilities in Kernel components, the most severe vulnerability in this section could lead to local escalation of privilege in system libraries with no additional execution privileges needed.(CVE-2022-0847, CVE-2022-20009, CVE-2022-20008, CVE-2021-22600)
- Multiple high severity vulnerabilities in MediaTek telephony and ion components. (CVE-2022-20084, CVE-2022-20109, CVE-2022-20110)
- Multiple high severity vulnerabilities in Qualcomm WLAN, Kernel and Display components. (CVE-2022-22057, CVE-2022-22064, CVE-2022-22065, CVE-2022-22068, CVE-2022-22072)
- Multiple high and critical severity vulnerabilities in Qualcomm closed-source components. (CVE-2021-35090, CVE-2021-35072, CVE-2021-35073, CVE-2021-35076, CVE-2021-35078, CVE-2021-35080, CVE-2021-35086, CVE-2021-35087, CVE-2021-35094, CVE-2021-35096, CVE-2021-35116)

Successful exploitation of the most severe of these vulnerabilities could allow for escalation of privilege. 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:
We recommend the following actions 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/2022-05-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22600
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35072
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35073
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35076
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35078
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35080
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35086
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35087
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35094
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35096
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39662
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39662
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39670
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39700
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20084
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20109
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20110
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20112
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20114
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20115
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20116
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22057
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22064
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22065

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22068
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22072