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:
06/07/2022

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Android 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. Depending on the privileges associated with the exploited component, an attacker could then install programs; view, change, or delete data; or create new accounts with full rights.

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

SYSTEMS AFFECTED:

- Android OS patch levels prior to 2022-06-05

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 in the context of the affected component. Following the MITRE ATT&CK framework, exploitation of these vulnerabilities can be classified as follows:

Tactic: *Initial Access* (TA0001):

Technique: *Drive-by Compromise* (T1189):

- A vulnerability in System that could lead to arbitrary code execution with no additional execution privileges needed. (CVE-2022-20127)
- A vulnerability in Media Framework that could lead to arbitrary code execution with no additional execution privileges needed. (CVE-2022-20130)

Tactic: *Privilege Escalation* (TA0029):

Technique: *Exploitation for Privilege Escalation* (T1404):

- Multiple vulnerabilities in System that could lead to local escalation of privilege with no additional execution privileges needed. (CVE-2022-20140, CVE-2022-20145)

Tactic: *Impact* (TA0040):

Technique: *Endpoint Denial of Service: Application or System Exploitation* (T1499):

- A vulnerability in Unisoc components that could allow for denial of service. (CVE-2022-20210)

Details of lower-severity vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could lead to local escalation of privilege with no additional execution privileges needed. (CVE-2021-39691, CVE-2022-20006, CVE-2022-20125, CVE-2022-20138)
- Multiple vulnerabilities in System that could lead to escalation of privilege. (CVE-2022-20124, CVE-2022-20126, CVE-2022-20133, CVE-2022-20134, CVE-2022-20135, CVE-2022-20137, CVE-2022-20142, CVE-2022-20144, CVE-2022-20147)
- Multiple vulnerabilities in System that could lead to information disclosure. (CVE-2022-20123, CVE-2022-20131)
- Multiple vulnerabilities in System that could lead to denial of service. (CVE-2021-39624, CVE-2022-20210, CVE-2022-20129, CVE-2022-20143)
- Multiple vulnerabilities in Kernel components that could lead to local escalation of privilege with no additional execution privileges needed. (CVE-2021-4154, CVE-2022-20141, CVE-2022-24958, CVE-2022-25258)
- Multiple vulnerabilities in Kernel components that could lead to information disclosure. (CVE-2022-20132, CVE-2022-20136)
- A vulnerability in MediaTek WIFI Firmware components. (CVE-2022-21745)

- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2021-35083, CVE-2021-35102, CVE-2021-35111, CVE-2022-22082, CVE-2022-22083, CVE-2022-22084, CVE-2022-22085, CVE-2022-22086, CVE-2022-22087, CVE-2022-22090)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the exploited component, an attacker could then install programs; view, change, or delete data; or create new accounts with full rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate updates provided by Google or mobile carriers to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- 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. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

REFERENCES:

Google:
https://source.android.com/security/bulletin/2022-06-01

The Hacker News:
https://thehackernews.com/2022/06/critical-unisoc-chip-vulnerability.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4154
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35083
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35102
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35111
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39624
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39691
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20123
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20124
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20125
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20126
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20127
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20129
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20130
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20131
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20132
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20133
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20134
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20135
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20136
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20137
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20138
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20140
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20141
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20142
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20145
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20147
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20210
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22082
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22083
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22084
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22085
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22086
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22087
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24958
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25258