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:
08/02/2022

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Android 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 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 2022-08-05

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 remote 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 remote code execution over Bluetooth with no additional execution privileges needed. (CVE-2022-20345)

Details of lower-severity vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could lead to local information disclosure with no additional execution privileges needed.(CVE-2021-39696, CVE-2022-20344, CVE-2022-20348, CVE-2022-20349, CVE-2022-20356)
- Multiple vulnerabilities in Framework that could lead to information disclosure. (CVE-2022-20350, CVE-2022-20352, CVE-2022-20357, CVE-2022-20358)
- Multiple vulnerabilities in Media Framework that could lead to remote information disclosure with no additional execution privileges needed. (CVE-2022-20346, CVE-2022-20353)
- Multiple vulnerabilities in System that could lead to escalation of privilege. (CVE-2022-20347, CVE-2022-20354, CVE-2022-20360, CVE-2022-20361)
- A vulnerability in System that could lead to Denial of Service. (CVE-2022-20355)
- A vulnerability in Kernel components that could lead to escalation of privilege. (CVE-2022-1786)
- Multiple vulnerabilities in Imagination Technologies components. (CVE-2021-0698, CVE-2021-0887, CVE-2021-0891, CVE-2021-0946, CVE-2021-0947, CVE-2021-39815, CVE-2022-20122)
- Multiple vulnerabilities in MediaTek components. (CVE-2022-20082)
- Multiple vulnerabilities in Unisoc components. (CVE-2022-20239)
- Multiple vulnerabilities in Qualcomm components. (CVE-2022-22080)
- Multiple vulnerabilities in Qualcomm components Closed-source components. (CVE-2021-30259, CVE-2022-22059, CVE-2022-22061, CVE-2022-22062, CVE-2022-22067, CVE-2022-22069, CVE-2022-22070, CVE-2022-25668)

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 7.2 : Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **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.
    - **Safeguard 9.1 : Ensure Use of Only Fully Supported Browsers and Email Clients:** Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
    - **Safeguard 18.3 : Remediate Penetration Test Findings**: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
    - **Safeguard 18.5 : Perform Periodic Internal Penetration Tests:** Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.
- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.
    - **Safeguard 2.3 : Address Unauthorized Software**: Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
    - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
    - **Safeguard 9.3 : Maintain and Enforce Network-Based URL Filters**: Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6 : Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise's email gateway.
- 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/2022-08-01

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20345
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20344
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20348
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20349
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20356
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20350
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20352
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20357
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20358
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20346
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20353
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20347
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20354
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20360
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20361
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20355
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1786
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0698
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0887
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0947
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39815
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20122
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20082
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20239
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22080
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30259

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22059
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22062
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22067
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22069
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22070
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25668