

*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](http://www.cisa.gov/tlp)

**Information may be distributed without restriction, subject to standard copyright rules.**

**DATE(S) ISSUED:**

09/07/2022

**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 remote 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 2022-09-05

**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:** *Execution* (TA0002):

**Technique:** *Exploitation for Client Execution* (T1203):

- A vulnerability in MediaTek components BT firmware could result in remote code execution due to a missing bounds check. User interaction is not needed for exploitation. No exploitation of this vulnerability has been observed in the wild. (CVE-2022-26447)

Details of lower-severity vulnerabilities are as follows:

- Multiple vulnerabilities in Android runtime that could allow for escalation of privilege. (CVE-2022-22822, CVE-2022-23852, CVE-2022-23990, CVE-2022-25314)
- Multiple vulnerabilities in Framework that could allow for escalation of privilege. (CVE-2022-20218, CVE-2022-20392, CVE-2022-20197)
- Multiple vulnerabilities in Framework that could allow for information disclosure. (CVE-2022-20393, CVE-2020-0500)
- Multiple vulnerabilities in System that could allow for escalation of privilege. (CVE-2022-20395, CVE-2022-20398)
- A vulnerability in System that could allow for information disclosure. (CVE-2022-20396)
- Multiple vulnerabilities in Kernel that could allow for information disclosure. (CVE-2022-20399, CVE-2022-23960)
- Multiple vulnerabilities in Kernel components that could allow for escalation of privilege. (CVE-2021-4083, CVE-2022-29582)
- Multiple vulnerabilities in Imagination Technologies components. (CVE-2021-0697, CVE-2021-0942, CVE-2021-0943, CVE-2021-0871)
- Multiple vulnerabilities in Unisoc components. (CVE-2022-20385, CVE-2022-20386, CVE-2022-20387, CVE-2022-20388, CVE-2022-20389, CVE-2022-20390, CVE-2022-20391)
- Multiple vulnerabilities in Qualcomm components. (CVE-2022-22095, CVE-2022-25656, CVE-2022-25670, CVE-2022-25693, CVE-2022-25704, CVE-2022-25706)
- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2022-25708, CVE-2022-22066, CVE-2022-22074, CVE-2022-22081, CVE-2022-22089, CVE-2022-22091, CVE-2022-22092, CVE-2022-22093, CVE-2022-22094, CVE-2022-25669, CVE-2022-25686, CVE-2022-25688, CVE-2022-25690, CVE-2022-25696)

Successful exploitation of the most severe of these vulnerabilities could allow for remote 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 patches provided by Google 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**)
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
  - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Apple® System Integrity Protection (SIP) and Gatekeeper™.

## REFERENCES:

### Google:

<https://source.android.com/docs/security/bulletin/2022-09-01>

### CVE:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0500>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0697>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0871>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0942>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0943>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4083>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20197>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20218>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20385>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20386>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20387>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20388>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20389>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20390>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20391>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20392>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20393>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20395>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20396>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20398>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20399>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22066>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22074>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22081>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22089>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22091>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22092>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22093>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22094>  
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22095>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22822>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23852>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23960>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23990>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25314>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25656>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25669>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25670>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25686>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25688>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25690>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25693>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25696>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25704>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25706>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25708>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26447>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29582>