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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
09/08/2021

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 September 5, 2021.

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **Medium**
- Small business entities: **Medium**

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 within the context of a privileged process. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities in Framework that could enable a remote attacker using a specially crafted file to cause a permanent denial of service. (CVE-2021-0595, CVE-2021-0683, CVE-2021-0684, CVE-2021-0685, CVE-2021-0687, CVE-2021-0688)
- Multiple vulnerabilities in Media Framework that could enable a local malicious application to bypass operating system protections that isolate application data from other applications. (CVE-2021-0689, CVE-2021-0690)
- Multiple vulnerabilities in System that could enable a local attacker using a specially crafted transmission to gain access to additional permissions. (CVE-2021-0428, CVE-2021-0598, CVE-2021-0644, CVE-2021-0682, CVE-2021-0691, CVE-2021-0692, CVE-2021-0693)
- A vulnerability in Kernel components could enable a local malicious application to bypass operating system protections that isolate application data from other applications. (CVE-2021-0695)
- Multiple high severity vulnerabilities in MediaTek Components. (CVE-2021-0680, CVE-2021-0681)
- Multiple high severity vulnerabilities in Unisoc Components. (CVE-2021-0635, CVE-2021-0636)
- Multiple high severity vulnerabilities in Qualcomm components. (CVE-2021-1941, CVE-2021-1948, CVE-2021-1974, CVE-2021-30290, CVE-2021-30294)
- Multiple critical and high severity vulnerabilities in Qualcomm closed-source components (CVE-2021-1886, CVE-2021-1888, CVE-2021-1889, CVE-2021-1890, CVE-2021-1933, CVE-2021-1946, CVE-2021-1909, CVE-2021-1923, CVE-2021-1934, CVE-2021-1935, CVE-2021-1952, CVE-2021-1971, CVE-2021-30295)

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/2021-09-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0595
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0683
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0684
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0685

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0687
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0688
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0689
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0690
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0428
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0598
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0682
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0691
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0692
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0693
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0695
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0680
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0681
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0635
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1941
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1948
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30290
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30294
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1886
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1888
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1933
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1923
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1934
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1935
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30295

TLP: WHITE

https://www.cisa.gov/tlp