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:
11/02/2021

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 indications that CVE-2021-1048 may be under limited, targeted exploitation.

SYSTEMS AFFECTED:

- Android OS builds utilizing Security Patch Levels issued prior to November 6, 2021.

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

- Multiple vulnerabilities in Framework that could enable a local attacker to gain access to additional permissions with no user interaction required. (CVE-2021-0799, CVE-2021-0921,

CVE-2021-0923, CVE-2021-0926, CVE-2021-0933, CVE-2020-13871, CVE-2021-0653, CVE-2021-0922)
- A vulnerability in Media Framework that could enable a local malicious application to bypass user interaction requirements in order to gain access to additional permissions. (CVE-2021-0928, CVE-2021-0650)
- Multiple vulnerabilities in System could enable a remote attacker using a specially crafted transmission to execute arbitrary code within the context of a privileged process. (CVE-2021-0918, CVE-2021-0930, CVE-2021-0434, CVE-2021-0649, CVE-2021-0932, CVE-2021-0925, CVE-2021-0931, CVE-2021-0919)
- Multiple vulnerabilities in Project Mainline components. (CVE-2021-0653, CVE-2021-0650, CVE-2021-0649)
- Multiple vulnerabilities in Kernel components that could result in local escalation of privilege due to a use after free. (CVE-2021-0920, CVE-2021-0924, CVE-2021-0929, CVE-2021-1048)
- Multiple vulnerabilities in Android TV that could enable a proximate attacker to silently pair with a TV and execute arbitrary code with no privileges or user interaction required. (CVE-2021-0889, CVE-2021-0927)
- A high severity vulnerability in MediaTek components. (CVE-2021-0672)
- Multiple critical severity vulnerabilities in Qualcomm closed-source components. (CVE-2021-1924, CVE-2021-1975)
- Multiple high severity vulnerabilities in Qualcomm closed-source components. (CVE-2021-1921, CVE-2021-1973, CVE-2021-1979, CVE-2021-1981, CVE-2021-1982, CVE-2021-30254, CVE-2021-30255, CVE-2021-30259, CVE-2021-30284)

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/2021-11-01#2021-11-06-security-patch-level-vulnerability-details

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0649

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0653
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0672
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0919
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0921
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0922
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0923
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0924
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0925
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0928
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0929
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0930
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0932
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0933
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1921
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1924
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1979
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30254
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30255
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30259
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30284

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.