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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/07/2019

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

OVERVIEW:
Multiple vulnerabilities have been discovered in the Google Android operating system (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 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 August 5, 2019.

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: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Android OS, the most severe of which could allow for arbitrary code execution within the context of a privileged process. Details of these vulnerabilities are as follows:

- An arbitrary code vulnerability in Broadcom components. (CVE-2019-11516)
- An arbitrary code vulnerability in Media framework. (CVE-2019-2126)
- An arbitrary code vulnerability in System. (CVE-2019-2130)

- An elevation of privilege vulnerability in Android runtime. (CVE-2019-2120)
- An information disclosure vulnerability in Media framework. (CVE-2019-2129)
- A denial of service vulnerability in System component. (CVE-2019-2137)
- Multiple elevation of privilege vulnerabilities in Framework. (CVE-2019-2121, CVE-2019-2122, CVE-2019-2125)
- Multiple elevation of privilege vulnerabilities in Media framework. (CVE-2019-2127, CVE-2019-2128)
- Multiple elevation of privilege vulnerabilities in System. (CVE-2019-2131, CVE-2019-2132, CVE-2019-2133, CVE-2019-2134)
- Multiple information disclosure vulnerabilities in System. (CVE-2019-2135, CVE-2019-2136)
- Multiple vulnerabilities in Qualcomm components. (CVE-2019-10492, CVE-2019-10499, CVE-2019-10509, CVE-2019-10510, CVE-2019-10538)
- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2019-2294, CVE-2019-10489, CVE-2019-10539, CVE-2019-10540)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of a privileged process. These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files. Depending on the privileges associated with the 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/2019-08-01.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2120
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2121
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2122
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2125
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2126
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2127
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2128
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2129
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2130

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2131
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2132
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2133
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2134
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2135
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2136
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2137
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2294
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10489
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10492
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10499
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10509
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10510
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10538
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10539
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10540
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11516

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov