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.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/02/2019

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 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 April 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 elevation of privilege vulnerability in Framework. (CVE-2019-2026)
- Multiple arbitrary code execution vulnerabilities in Media framework. (CVE-2019-2027, CVE-2019-2028)
- An arbitrary code execution vulnerability in System. (CVE-2019-2029)
- Multiple elevation of privilege vulnerabilities in System. (CVE-2019-2030, CVE-2019-2031, CVE-2019-2033, CVE-2019-2034, CVE-2019-2035, CVE-2019-2032, CVE-2019-2041)
- Multiple information disclosure vulnerabilities in System. (CVE-2019-2037,CVE-2019-2038, CVE-2019-2039, CVE-2019-2040)
- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2018-11271, CVE-2018-11291, CVE-2018-11821, CVE-2018-11822, CVE-2018-11828, CVE-2018-11849, CVE-2018-11850, CVE-2018-11853, CVE-2018-11854, CVE-2018-11856, CVE-2018-11859, CVE-2018-11861, CVE-2018-11862, CVE-2018-11867, CVE-2018-11870, CVE-2018-11871, CVE-2018-11872, CVE-2018-11873, CVE-2018-11874, CVE-2018-11875, CVE-2018-11876, CVE-2018-11877, CVE-2018-11879, CVE-2018-11880, CVE-2018-11882, CVE-2018-11884, CVE-2018-11928, CVE-2018-11936, CVE-2018-11967, CVE-2018-11968, CVE-2018-11976, CVE-2018-12004, CVE-2018-12005, CVE-2018-12012, CVE-2018-12013, CVE-2018-13885, CVE-2018-13886, CVE-2018-13887, CVE-2018-13895, CVE-2018-13925, CVE-2019-2244, CVE-2019-2245, CVE-2019-2250)
- Multiple vulnerabilities in Qualcomm components. (CVE-2017-17772, CVE-2018-11294, CVE-2018-11299, CVE-2018-11826, CVE-2018-11827, CVE-2018-11840, CVE-2018-11851, CVE-2018-11860, CVE-2018-11868, CVE-2018-11869, CVE-2018-11878, CVE-2018-11889, CVE-2018-11891, CVE-2018-11894, CVE-2018-11895, CVE-2018-11897, CVE-2018-11902, CVE-2018-11904, CVE-2018-11905, CVE-2018-11923, CVE-2018-11924, CVE-2018-11925, CVE-2018-11927, CVE-2018-11930, CVE-2018-11937, CVE-2018-11940, CVE-2018-11949, CVE-2018-11953, CVE-2018-13920, CVE-2018-5855)

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/2019-04-01

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17772
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5855
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11271
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11291
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11294
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11299
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11821
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11822
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11826
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11827
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11828
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11840
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11849
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11850
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11851
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11853
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11854
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11856
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11859
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11860
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11861
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11862
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11867
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11868
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11869
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11870
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11871
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11872
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11873

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11874
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11875
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11876
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11877
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11878
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11879
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11880
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11882
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11884
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11889
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11891
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11894
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11895
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11897
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11902
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11904
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11905
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11923
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11924
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11925
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11927
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11928
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11930
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11936
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11937
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11940
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11949
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11953
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11967
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11968
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11976
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12004
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12005
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12012
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13885
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13886
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13887
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13895
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13920
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13925
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2026
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2027

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2028
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2029
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2030
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2031
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2032
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2033
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2034
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2035
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2037
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2038
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2039
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2040
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2041
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2244
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2245
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2250