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:

07/02/2019

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 July 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 System. (CVE-2019-2111)
- An information disclosure vulnerability in Framework. (CVE-2019-2104)
- Multiple arbitrary code vulnerabilities in Library. (CVE-2019-2105)
- Multiple arbitrary code vulnerabilities in Media framework. (CVE-2019-2106, CVE-2019-2107, CVE-2019-2109)
- Multiple elevation of privilege vulnerabilities in System. (CVE-2019-2112, CVE-2019-2113)
- Multiple information disclosure vulnerabilities in System. (CVE-2019-2116, CVE-2019-2117, CVE-2019-2118, CVE-2019-2119)
- Multiple vulnerabilities in Qualcomm closed-source components. (CVE-2019-2235, CVE-2019-2236, CVE-2019-2237, CVE-2019-2238, CVE-2019-2239, CVE-2019-2240, CVE-2019-2241, CVE-2019-2253, CVE-2019-2254, CVE-2019-2322, CVE-2019-2327, CVE-2019-2334, CVE-2019-2346)
- Multiple vulnerabilities in Qualcomm components. (CVE-2019-2276, CVE-2019-2278, CVE-2019-2305, CVE-2019-2307, CVE-2019-2308, CVE-2019-2330, CVE-2019-2326, CVE-2019-2328)

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/2019-07-01.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2104

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2105

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2106

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2107

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2109

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2111

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2112

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2113

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2116

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2117

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2118

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2119

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2235

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2236

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2237

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2238

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2239

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2240

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2241

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2253

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2254

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2276

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2278

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2305

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2307

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2308

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2322

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2326

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2327

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2328

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2330

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2334

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2346

Ryan Thomas
Security Operations Analyst
MS Department of Information Technology Services
601-432-8032 | www.its.ms.gov

Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381