MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Google Android OS Could Allow for Arbitrary Code Execution

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2019-059

DATE(S) ISSUED:
06/04/2019

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 June 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:

- Multiple vulnerabilities in Framework could allow for escalation of privilege (CVE-2019-2090, CVE-2019-2091, CVE-2019-2092).

- A vulnerability in Framework could allow for information disclosure (CVE-2018-9526).
- Multiple vulnerabilities in Media framework that could allow for arbitrary code execution (CVE-2019-2093, CVE-2019-2094, CVE-2019-2095).
- A vulnerability in Media framework that could allow for escalation of privilege (CVE-2019-2096).
- A vulnerability in System that could allow for arbitrary code execution (CVE-2019-2097).
- Multiple vulnerabilities in System that could allow for escalation of privilege (CVE-2019-2102, CVE-2019-2098, CVE-2019-2099).
- A vulnerability in Kernel components could allow for information disclosure (CVE-2019-2101).
- Multiple High severity vulnerabilities in Qualcomm components (CVE-2019-2260, CVE-2019-2292).
- Multiple Critical severity vulnerabilities in Qualcomm components (CVE-2019-2269, CVE-2019-2287).
- Multiple Critical severity vulnerabilities in Qualcomm closed-source components (CVE-2018-13924, CVE-2018-13927).
- Multiple High severity vulnerabilities in Qualcomm closed-source components (CVE-2018-13896, CVE-2019-2243, CVE-2019-2261).

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:
We recommend the following actions 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/2019-06-01

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13896
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13924
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2091

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2092
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2093
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2094
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2095
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2096
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2097
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2098
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2099
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2101
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2102
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2243
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2260
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2261
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2269
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2287
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2292

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722