Alert – Multiple vulnerabilities in the Google Android operating system (OS)

Description

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.

Impact of the vulnerabilities

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.

Vulnerable or affected version:

- Android OS builds utilizing Security Patch Levels issued prior to May 5, 2019

Risk:

- All Government and Business entities which run Google Android OS, the risk is **High**.

Details of these vulnerabilities are as follows:

- A vulnerability in Framework could allow for escalation of privilege (CVE-2019-2043).
- Multiple vulnerabilities in Media framework that could allow for remote code execution (CVE-2019-2044).
- Multiple vulnerabilities in System that could allow for remote code execution (CVE-2019-2045, CVE-2019-2046, CVE-2019-2047).
- Multiple vulnerabilities in System that could allow for escalation of privilege (CVE-2019-2049, CVE-2019-2050).
- Multiple vulnerabilities in System that could allow for information disclosure (CVE-2019-2051, CVE-2019-2052, CVE-2019-2053).
- A vulnerability in Kernel components could allow for escalation of privilege (CVE-2019-2054).
- A vulnerability in NVIDIA components could allow for escalation of privilege (CVE-2018-6243).
- A vulnerability in Broadcom components could allow for remote code execution (CVE-2018-19860)
- Multiple High severity vulnerabilities in Qualcomm components (CVE-2018-11955, CVE-2018-13919).

These vulnerabilities could be exploited through multiple methods such as email, web browsing, and MMS when processing media files.

Solutions (Mitigations):

Rw-CSIRT is strongly recommending **users** and **IT administrators** to follow the instructions below:

- 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.

Affected users should: contact Rw-CSIRT by calling us on **4045** or writing to **security@risa.rw**

References from google Android:

https://source.android.com/security/bulletin/2019-05-01

Vulnerabilities Details:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5912
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5913
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6243
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-11955
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13901
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13902
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13907
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13911
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13919
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19860
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2045
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2046
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2050
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2051
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2053
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2054
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2255
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2256

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of “early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability” and raise cyber security awareness in public.