

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-108

DATE(S) ISSUED: 10/03/2018

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 remote 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 remote 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 October 1, 2018.

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 remote code execution within the context of a privileged process. Details of these vulnerabilities are as follows:

- A denial of service vulnerability in Framework. (CVE-2018-9452)
- Multiple elevation of privilege vulnerabilities in Framework. (CVE-2018-9490, CVE-2018-9492)
- An information disclosure vulnerability in Framework. (CVE-2018-9493)
- A remote code vulnerability in Framework. (CVE-2018-9491)
- An information disclosure vulnerability in Media Framework. (CVE-2018-9499)
- Multiple remote code vulnerabilities in Media Framework. (CVE-2018-9473, CVE-2018-9496, CVE-2018-9497, CVE-2018-9498)
- Multiple information disclosure vulnerabilities in System. (CVE-2018-9502, CVE-2018-9503, CVE-2018-9505, CVE-2018-9506, CVE-2018-9507, CVE-2018-9508, CVE-2018-9509, CVE-2018-9510)
- Multiple remote code vulnerabilities in System. (CVE-2017-13283, CVE-2018-9504)
- A denial of service vulnerability in System. (CVE-2018-9511)
- Multiple elevation of privilege vulnerabilities in System. (CVE-2018-9476, CVE-2018-9501)
- Multiple elevation of privilege vulnerabilities in Kernel components. (CVE-2018-9513, CVE-2018-9514, CVE-2018-9515)

Successful exploitation of the most severe of these vulnerabilities could allow for remote 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, when they become available.
- 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/2018-10-01.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13283>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9473>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9496>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9497>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9498>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9499>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9476>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9504>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9501>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9502>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9503>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9505>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9506>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9507>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9508>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9509>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9510>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9511>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9513>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9514>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9515>

24x7 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



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/>