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.

There are currently no reports of these vulnerabilities being exploited in the wild.


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

- A vulnerability in Media framework that could allow for escalation of privilege (CVE-2019-2096).
- A vulnerability in Kernel components could allow for information disclosure (CVE-2019-2101).

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:

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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/