UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00089

CRITICAL ANDROID RCE BUG

DATE ISSUED: 12th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A security update from Google has addressed 43 bugs affecting Android mobile phones, including the likes of giants such as Samsung in their latest security release.

BREAKDOWN

In addition to the 43 bugs addressed by Google this month in their patch release, Qualcomm have patched 15 flaws identified as critical and high severity for their chipsets used in Android mobile phones. Critical severity flaw CVE-2021-0316 allowed Remote Code Execution (RCE) in the Google Android System component, while CVE-2021-0313 can cause denial of service issues. Versions 8.0, 8.1, 9, 10 and 11 are protected once the latest patches are applied. For a full list of vulnerabilities, see the references below.

REMEDIATION STEPS

- Employ endpoint protection on all mobile devices such as anti-malware software.
- Install updates and security patches when they become available – ensure mobile devices are set to automatically check for updates at regular intervals in the device settings.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/google-warns-of-critical-android-remote-code-execution-bug/162756/
Cyber Security News https://thecybersecurity.news/vulnerabilities/google-warns-of-critical-android-remote-code-execution-bug-4944/