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

CYBER GUIDANCE ISSUE 00019

ACHILLES QUALCOM SNAPDRAGON SECURITY EXPLOIT

DATE ISSUED: 7th August 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	LOW	MEDIUM	HIGH

OVERVIEW

40% of all android smartphones rely on the Qualcomm Snapdragon processors and Checkpoint researchers have discovered 400 vulnerabilities within the Digital Signal Processor (DSP) that processes real-time requests in the SoC's Hexagon architecture chipsets.

BREAKDOWN

The vulnerabilities have been grouped into six CVE exploits that are being collectively known as Achilles, enabling the device to be used for exfiltration of photographs, videos, real-time GPS information and microphone data. Malware may be discretely positioned on the devices, making it difficult to detect and remove, as well as facilitating targeted Denial of Service (DoS) and privilege escalation attacks. Affected vendors include Google, Samsung, LG, Xiomi and OnePlus. In order to be susceptible to the exploit, users must first download and run a rogue executable.

CVE-2020-11201, CVE-2020-11202, CVE-2020-11206, CVE-2020-11207, CVE-2020-11208 and CVE-2020-11209

REMEDIATION STEPS

- Apply patches released by Qualcomm for all six exploits and vendor software updates
- Factory reset any affected devices

REFERENCES & RESOURCES

Checkpoint https://blog.checkpoint.com/2020/08/06/achilles-small-chip-big-peril/
Hot Hardware: https://hothardware.com/news/millions-of-android-phones-vulnerable-to-achilles-qualcomm-snapdragon-security-expoits
Threatpost: https://threatpost.com/qualcomm-bugs-opens-40-percent-of-android-devices-to-attack/158194/