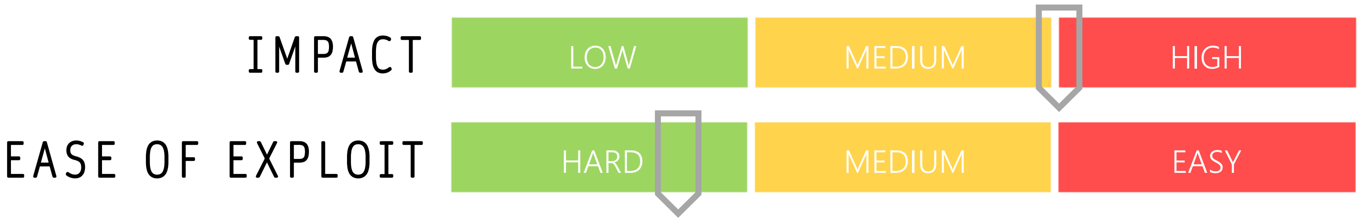
UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00155

INTEL FIXES 73 BUGS IN CPU FIRMWARE

DATE ISSUED: 14th June 2021



OVERVIEW

Most of the vulnerabilities in the popular Intel CPUs are being discovered in-house by conducting due diligence checks, but BIOS firmware in the chipsets are difficult to patch and even more difficult to exploit, however could prove to be a juicy target to a savvy attacker.

BREAKDOWN

The 29 patches released by Intel cover 73 known vulnerabilities in the popular processors with 55% having been discovered internally and the remainder as part of the bug-bounty program. The vulnerabilities affected graphics, networking and Bluetooth components and have been mitigated before public disclosure took place. The highest rating was 8.8 for a network-exploitable privilege escalation bug affecting NUC computers, the Drivery and Support Assistant (DSA) and the RealSense ID platform and potential Denial of Service (DoS) in some Thunderbolt controllers CVE-2021-24489. The four receiving a 7.5 rating relate to improper initialisation, race condition, improper input validation and insufficient control flow management. CVE-2020-12357, CVE-2020-8670, CVE-2020-8700 & CVE-2020-12359. CVE-2021-0133 was given a CVSS rating of 7.7 and affects iterations of versions prior to 3.3 that affects the Intel Security Library and may lead to privilege escalation for authenticated attackers over network access, DoS and system information disclosure.

REMEDIATION STEPS

- Apply patches where possible.
- Restrict user privileges on shared devices and network accessible devices.
- Use NIST and CIS frameworks and guidelines to deploy security in depth across the network at all levels, not just at the perimeter.

REFERENCES & RESOURCES

Intel	https://www.intel.com/content/www/us/en/security-center/default.html
Threatpost	https://threatpost.com/intel-security-holes-cpus-bluetooth-security/166747/