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

CYBER GUIDANCE ISSUE 00228

INTEL SECURITY BUG EXPOSES ENCRYPTION KEYS

DATE ISSUED: 23rd November 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Positive Technologies have discovered a security flaw in Intel Chipsets in a debugging functionality that has unnecessary privileges giving an attacker the potential ability to access encrypted files, bypass copyright protections on digital content snoop to their hearts content.

BREAKDOWN

Now being tracked as CVE-2021-0146 and rated 7.1/10 on the CVSS vulnerability severity scale, using the test or debug logic at runtime, an attacker may be able to gain unauthenticated access by extracting the encryption key and elevate their privileges. This attack is possible with physical device access. The vulnerability is known to affection Pentium. Atom, and Celeron processors release with Apollo Lake and Gemini Lake which are used in mobile devices, laptops, medical devices IoT devices, and embedded systems. It is also possible to extract the root encryption key used to protect digital content and is used across Intel's Platform Trust Technology and Enhanced Privacy ID technologies e.g. electronic books (E-Books).

REMEDIATION STEPS

- Install the UEFI BIOS updates published by manufacturer. You can find a full list in the resources below.

REFERENCES & RESOURCES

Intel	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00528.html
Threatpost	https://threatpost.com/intel-processor-bug-encryption-keys/176355/
CVE-Mitre	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0146