UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00121

NEW INTEL SIDE CHANNEL ATTACKS

DATE ISSUED: 15th March 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	[✓ HARD]	MEDIUM	EASY

OVERVIEW

A new kind of side channel attack has been discovered that affects Intel CPU's by taking advantage of the interconnect contention in the CPU Ring, rather than leveraging shared memory or cache like traditional side channel attacks in order to exfiltrate sensitive information, such as cryptographic keys.

BREAKDOWN

Previously side-channel attacks have relied on memory and cache vulnerabilities, but this new attack leverages the component that facilitates communication across various components of the CPU itself including cores, system agents and graphics units in Intel Processors such as the Skylake and Coffee Lake models. A skilled adversary could potentially glean "key bits" using the precise keystrokes of a victim user by exploiting vulnerable cryptographic implementations. In order to do this, the attacker must have already compromised the machine in question and have the ability to run "unprivileged code" to run malware, steal credentials and execute scripts or code. This type of attack was discovered by a team of researchers at the University of Illinois. It is unclear at this stage how feasible this type of attack may be.

REMEDIATION STEPS

- N/A: Further research and investigation required.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/intel-side-channel-attack-data/164582/
University of Illinois	https://arxiv.org/pdf/2103.03443.pdf