Alcatel-Lucent Security Advisory No. SA-C0061 Ed. 02

Information on MELTDOWN and SPECTRE vulnerabilities for Communications portfolio

Summary

Two vulnerabilities called Meltdown and Spectre, have been discovered that exploit techniques, speculative execution and page table management, implemented in modern processors that could allow malicious programs to access information from the memory of other programs executing on the processor.

This Security Advisory provides information about ALE Communication portfolio, explaining that the risk on ALE products is rated low/medium with potential but minimal impact.

Edition 02 of the advisory addresses future integration of CPU microcode and operating system security upgrades on concerned products.

Description of Issue

Security researchers have discovered that CPU operations related to speculative execution and page table management can be abused to leak information leading to arbitrary virtual memory read vulnerabilities across local security boundaries in various contexts.

The following three variants of this issue are known to affect many modern processors, including certain processors by Intel, AMD and ARM

Spectre:

Variant 1: bounds check bypass	(CVE-2017-5753)
Variant 2: branch target injection	(CVE-2017-5715)

Meltdown:

Variant 3: rogue data cache load	(CVE-2017-5754)

Full details of the "Meltdown" and "Spectre" vulnerabilities can be found at the following URLs:

- https://meltdownattack.com/
- https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html

Risk evaluation on ALE products

ALE Communications products are based on different types of CPU, some of which based on the architectures that are concerned by the reported vulnerabilities. However, the required conditions to execute these vulnerabilities are not allowed in ALE products, i.e. it is not possible to install and then execute any arbitrary code or process that could leverage the attack techniques.

Although the vector attack conditions are not allowed, ALE products running as a virtual appliance under a hypervisor could be impacted if the hypervisor is vulnerable. Untrusted users could then have access to other guest systems running under the same hypervisor, and an attacker could be able to read memory from the concurrent virtual appliance where the ALE application is running. Please contact your virtualization vendor to determine whether updates are available.

Alcatel-Lucent Enterprise is aware of significant public discussion of this issue and its related impact on systems performance. Proof of concept code has been published, but none of the published code is directly applicable to Alcatel-Lucent Enterprise products.

Considering the attack expertise (skilled) and requirements (access with account), the risk level of these vulnerabilities is rated as low/medium for ALE Communications products.

Recommended actions

Customers of ALE Communications products are reminded to ensure that access to their products is secured with management roles assigned to minimum required personnel, and to follow recommend security installation measures and configuration.
ALE recommends applying security updates as soon as they are available.

As part of a defense-in-depth strategy, Alcatel-Lucent Enterprise will continue to investigate kernel patches and CPU microcode updates for applications and platforms, and released them for each concerned product over time with a specific attention to their effectiveness. The status of security updates at the date of publication remains unstable, controversies remain open on the effectiveness of the first delivered security fixes as well as potential impacts on performance.
This advisory will be updated with the corresponding information as soon as available.

Status on Alcatel-Lucent Enterprise Communication Products

As stated, ALE application software and platforms are not directly vulnerable to these issues, but are running on environments that embed vulnerable CPU. All products, applications and solutions are then under investigation for ensuring the best level of multi-layered security.

ALE will release security updates for the CPU vulnerabilities so that they are not leveraged by any other exploits relying on arbitrary code execution.

Devices

Deskphones are closed systems that do not allow external code execution. Deskphones and accessories are not concerned by vulnerable CPU, with the only exception of 8088 Smart Deskphone in SIP mode only that is under investigation.

Platforms

Although required attack conditions are not allowed, the various products of following ALE Solutions families are potentially impacted and will need to receive operating systems and CPU microcode upgrade over time to mitigate any risk:

- OpenTouch Solutions
- OmniPCX Enterprise Solutions
- OmniPCX Office / OXO Connect solutions

For Rainbow cloud solutions, please refer to
https://support.openrainbow.com/hc/en-us/articles/115001995090-Security-Infrastructure-Meltdown-Spectre-vulnerabilities

Applications

ALE solutions running as virtual machines are potentially impacted in a shared environment, if the host allows running malicious code. Please contact your hypervisor supplier and apply related security updates, and install available security updates for the operating systems released for the corresponding products. This concerns:

- OpenTouch Solutions as a Virtual Machine
- OmniPCX Enterprise Solutions as a Virtual Machine
- OpenTouch Fax Center
- OmniTouch 8400 Instant Communication Suite

Communications Management and Security

- Omnivista 8770 Network Management system is Not affected. ALE however recommends applying related Microsoft Windows security updates.
- OpenTouch Session Border Controller is Not affected – ALE however recommends applying security updates of underlying hypervisors.

- IP Security Modules are potentially impacted, but with no capability to run arbitrary code on these closed products. Security updates are under investigation.

History

Ed.01 (2018 January 14th): creation

Ed.02 (2018 January 22nd): Products investigation status updates, impact analysis and product update strategy information.

This advisory will be updated with impact status and security updates availability regularly.