Security Bulletin for Mitel Open Integration Gateway

SECURITY BULLETIN ID: 18-0001-005

RELEASE VERSION: 1.0

DATE: 2018-07-17

OVERVIEW

This security bulletin provides product-specific details on the vulnerabilities described in Mitel Security Advisory 18-0001. Visit http://www.mitel.com/security-advisories for more details.

This Security Bulletin provides details and recommended solutions to address side channel analysis vulnerabilities, referred to as Spectre and Meltdown, impacting Mitel Open Integration Gateway (OIG).

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
OIG 3.0	OIG 3.0 with MSL 10.3.33.0	Upgrade to ServiceLink for MSL 10.3.45.0 and above (for 32 bit)
OIG 4.0	OIG 4.0 with MSL 10.5.15.0	Upgrade to ServiceLink for MSL 10.5.25.0 and above (for 64 bit)

RISK / EXPOSURE

This bulletin addresses the following vulnerabilities:

- Variant 1, Spectre, CVE-2017-5753, Bounds check bypass
- Variant 2, Spectre, CVE-2017-5715, Branch target injection
- Variant 3, Meltdown, CVE-2017-5754, Rogue data cache load

These vulnerabilities may allow unauthorized disclosure of sensitive information. The vulnerabilities are not expected to directly impact the integrity or availability of the system.

The risk due to this vulnerability is rated as low. Successful exploit requires an account with privileges to install code or a separate system compromise. Mitel Open Integration Gateway does not support installing custom software and is not directly vulnerable when running on a dedicated system with appropriate physical security and access control policies.

As a precautionary measure, Mitel is providing product updates for products that include the operating system in the Mitel provided software.

MITIGATION / WORKAROUNDS

There is no specific mitigation for these vulnerabilities.

SOLUTION INFORMATION

These issues are addressed in Service Link for MSL for Mitel Open Integration Gateway with 10.3.45.0 (32 bit) and 10.5.25.0 (64 bit) Releases. Customers are advised to upgrade to these releases.

Mitel
Powering connections

If operating in a virtual environment, hypervisor updates are required. Please consult guidance provided by your hypervisor supplier.

Customers also need to apply microcode updates for their specific processor. Please consult the guidance provided by your hardware supplier.

Mitigation of these issues requires patches from several vendors. These vendors have identified that such patches have the potential to impact performance of the systems following updates.

Mitel Open Integration Gateway is expected to meet published engineering guidelines when running on servers with the recommended minimum specifications, or in the case of virtual deployments, with the recommended virtual server reservations.

However, performance impacts will depend on the specific type and generation of microprocessor and the deployment specific work loads. Customers are cautioned that there may be performance impacts following patching and upgrades.

For further information, please contact Product Support.

Mitel®
Powering connections