Security Bulletin for MiVoice Business

SECURITY BULLETIN ID: 18-0001-002

RELEASE VERSION: 1.0

DATE: 2018-05-08

Mitel

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 MiVoice Business ISS and Virtual.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiVoice Business ISS and Virtual	8.0 SP3 (8.0.3.17) and earlier	Upgrade to 8.0 SP3 FP1 (8.0.3.24); Alternative for 8.0 thru 8.0 SP3 sites, upgrade ServiceLink for MSL to 10.5.25.0 or later from the Blades panel
MiVoice Business ICP3300 (all versions)	Not impacted	Not applicable

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. MiVoice Business 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.

Mitel
Powering connections

SOLUTION INFORMATION

These issues are addressed in product updates MiVoice Business SP3 FP1. Alternatively, for MiVoice Business 8.0 through 8.0 SP3, these issues may be addressed by an update to ServiceLink for MSL to MSL 10.5.25.0 or later.

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 internal testing has verified that after patches are applied, MiVoice Business continues 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 and are advised to monitor their systems following upgrades.

For further information, please contact Product Support.

Mitel
Powering connections