Security Bulletin for MiVoice Business Multi-Instance

SECURITY BULLETIN ID: 18-0001-007

RELEASE VERSION: 1.0

DATE: 2018-07-17

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 Multi-Instance.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiVoice Business Mult-Instance	2.0 SP1 (2.0.1.8) and earlier	Upgrade to R2.0SP1 and install ServiceLink upgrade to 10.3.45.0

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 Multi-Instance 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 operating system update ServiceLink 10.3.45.0, which can be installed on MiVoice Business 2.0 SP1. Customers are advised to install this update.

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

Mitel
Powering connections

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 Multi-Instance continues to meet published engineering guidelines when running on servers with the recommended minimum specifications.

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