Security Bulletin for MiVoice Border Gateway

SECURITY BULLETIN ID: 18-0001-006

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 MiVoice Border Gateway.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiVoice Border Gateway	9.3 and earlier	Upgrade to either R9.4 SP1 *or* R10.0 SP3. After either upgrade**,** install *ServiceLink 10.5.25.0* or later from the Blades panel.
MiVoice Border Gateway	9.4 PRx and 9.4 SP1 10.0 SP1, SP2, SP3	Install *ServiceLink 10.5.25.0* or later from the Blades panel.

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 Border 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 operating system update ServiceLink 10.5.25.0, which can be installed on any MiVoice Border Gateway R9.4 or R10.0 system. Customers are advised to install this update. For virtual deployments operating at or near capacity, customers may need to adjust virtual machine reservations to ensure peak load performance; further details are provided in the related Knowledge Management System article, SO3658.

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.

For deployments on industry standard servers (ISS), Mitel internal testing has verified that after updates are applied, the MiVoice Border Gateway continues to meet published engineering guidelines when running on servers with the recommended minimum specifications. These systems are typically constrained by I/O capacity and CPU performance is not a significant constraint.

For virtual deployments, Mitel internal testing has determined that in the scenario where systems are loaded to maximum capacity on hardware with CPU architecture Ivey Bridge and earlier (typically manufactured prior to 2014), customers should increase virtual machine reservations to ensure peak load performance. For systems operating well below maximum capacity, CPU performance impacts are less significant. Further details on procedures to assess and adjust CPU usage are available in the MiVoice Border Gateway Engineering Guidelines and related Knowledge Management System article.

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. Customers are advised to check CPU usage at peak load before and after patching.

For further information, please refer to the Product Support Knowledge Management System article, SO3658 available at https://mitel.custhelp.com/app/answers/answer_view/a_id/1010455, or contact Product Support.