Security Bulletin for MiVoice Office 400

SECURITY BULLETIN ID: 18-0001-008

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 Office 400.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiVoice Office 400 VA	R5.0 HF3 and earlier R4.1 HF6 and earlier	Release R5.0 HF4 will be available end of July 2018 Release R4.1 HF7 will be available end of July 2018
CPU2-S	Release 5.0.5.1 and earlier	Upgrade to Release 5.0.6.1; includes BIOS updates automatically applied by product update package
MiVoice Office 415, 430, 470 Controller	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 Office 400 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 MiVoice Office 400 VA Release R5.0 HF4, and R4.1 HF7 as well as in CPU2-S Release 5.0.6.1. Customers are advised to upgrade to these releases when available.

Mitel
Powering connections

For MiVoice Office 400 VA, 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.

For CPU2-S, plugged into MiVoice Office 470, BIOS updates will be applied by the product update package. Windows O/S updates will be provided through Windows update process.

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 Office 400 continues to meet published engineering guidelines when running 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