Security Bulletin for MiVoice MX-ONE

SECURITY BULLETIN ID: 18-0001-003

RELEASE VERSION: 1.0

DATE: 2018-05-08

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 MX-ONE and related products.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiVoice MX-ONE ISS and Virtual	6.1 thru 6.3 all SPs and HFs	Update to SLES11 SP4 or later
MiVoice MX-ONE Provisioning Manager	6.1 thru 6.3 all SPs and HFs	Update to SLES11 SP4 or later
MiVoice MX-ONE Media Server	6.1 thru 6.3 all SPs and HFs	Update to SLES11 SP4 or later
ASU II	6.1 thru 6.3 all SPs and HFs	Pending supplier updates
ASU Lite	6.1 thru 6.3 all SPs and HFs	Update CPU Bios to 80323T00 Update to SLES11 SP4 or later
ASU 4GB, ASU 8GB	6.1 thru 6.3 all SPs and HFs	Pending supplier updates
MGU2	Not impacted	Not applicable
MiVoice MX-ONE Express	6.1 thru 6.3 all SPs and HFs	Updates pending

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 MX-ONE 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.

Mitel
Powering connections

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 updates for SLES for MiVoice MX-ONE and related applications. Customers are advised to upgrade SLES to this release 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. For ASU-Lite, customers need to apply CPU bios updates in addition to the operating system updates, as listed in the table above.

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 MX-ONE 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 following patching and upgrades.

For further information, please refer to the Product Support Knowledge Management System article, RE1868, or contact Product Support.

Mitel
Powering connections