Security Bulletin for

MiCloud Management Portal

SECURITY BULLETIN ID: 18-0001-004

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 MiCloud Management Portal.

APPLICABLE PRODUCTS

This security bulletin provides information on the following products:

PRODUCT NAME	VERSIONS(S) AFFECTED	SOLUTIONS(S) AVAILABLE
MiCloud Management Portal	5.3 SP1 (5.3.112.0) and earlier	Install ServiceLink 10.5.25.0 or later from the Blades panel
MiCloud Management Portal	6.0 SP1 (6.0.135.0) and earlier	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. MiCloud Management Portal 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 includes the operating system in the Mitel provided software.

MITIGATION / WORKAROUNDS

Customers must upgrade their Mitel Standard Linux Operating System to address these vulnerabilities. No other mitigation/workarounds are available.

Mitel
Powering connections

SOLUTION INFORMATION

These issues are addressed in operating system update ServiceLink 10.5.25.0, which can be installed on Mitel Management Portal release 5.3 SP1 and 6.0 SP1. These issues are addressed in MiCloud Management Portal, Release 6.1. Customers are advised to upgrade to this release.

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, MiCloud Management Portal continues to meet the published engineering guidelines in case of virtual deployments, with the recommended virtual server reservations.

Performance impacts depend on the specific type and generation of microprocessor and the deployment specific workloads. Customers are cautioned that there may be performance impacts following patching and upgrades. Specifically, testing shows an increase in the import time duration which scales up with increase in the number of users. For more details, refer to *MiCloud Management Portal 6.1 Release Notes*.

For further information, please contact Product Support.

Mitel
Powering connections