Mitel Product Security Advisory 18-0001

Side-Channel Analysis Vulnerabilities

Advisory ID: 18-0001
Publish Date: 2018-01-08
Revision: 1.0

Summary

On January 3rd, 2018, researchers disclosed three vulnerabilities that leverage speculative execution capabilities of many modern processors. These vulnerabilities may allow unauthorized disclosure of information between different user processors and between user and kernel processes.

The vulnerabilities are referred to as Spectre (CVE-2017-5753, CVE-2017-5715) and Meltdown (CVE-2017-5754) that differ in the specific type of speculative execution exploited.

To successfully exploit these vulnerabilities, the attack vector requires malicious code executing on the same processor. Many Mitel products do not support installing custom software and are not directly vulnerable when running on dedicated systems. When running as a virtual machine in a shared hosting environment, Mitel products may be impacted by malicious code on the host.

Speculative execution is a capability to improve the performance of processors. As such, security updates to mitigate these vulnerabilities are expected to have performance penalties, the extent depending on the specific processor, operating system and application workload. Early results indicate performance benchmark testing, designed to stress specific processor components, may see negative performance impacts of 10 - 30%. These results are generally not representative of typical application workloads where various system bottlenecks constrain performance. The performance penalty is not expected to have a significant impact for most Mitel systems which operate well within their performance limits. Mitel is continuing to investigate performance impacts and will provide further information as available.

Security updates are being released by processor, operating system and virtualization providers. Early guidance indicates that server updates support tuneable configuration to allow a trade-off between security and performance. Customers concerned about performance impacts are

encouraged to review the available guidance and to assess the tradeoff between security exposure and performance impacts as applied to their own deployment environment.
Mitel recommends customers apply all available security updates as they become available. For Mitel products which include the underlying operating system, Mitel will be providing product updates.
Mitel is not aware of any active exploits of these vulnerabilities.

Mitel continues to investigate these vulnerabilities and information may change as the investigation continues. This advisory will be updated as information is available.

Products Under Investigation

All products are being evaluated for the impact of these vulnerabilities and the impact of released mitigations. This advisory will be updated with additional information as it becomes available.

Although Mitel application software is not directly affected, the underlying CPU vulnerability has the potential to increase the impact of other successful exploits that allow code execution. As such, as operating system providers release security updates, the relevant Mitel products will also be updated.

Risk Assessment

The risk of this vulnerability is rated as moderate to low for Mitel products.

Successful exploit requires an attacker to execute malicious code with user privileges, requiring an account with privileges to install code or a separate system compromise. Exploit of these vulnerabilities may expose confidential information but is not expected to directly impact the integrity or availability of the system.

Web browsers provide a vector for local code execution, such as JavaScript embedded in web pages. Such execution is normally contained by the browser but these vulnerabilities can potentially be exploited by this vector. Browser security updates have been or will soon be released for most common browsers.

Proof of concept code is publicly available. Mitel is not aware of active exploits.

Mitigation / Recommended Action

Customers are advised to follow good security practices including using caution when browsing to unknown and potentially malicious web sites. Specifically, customers are advised to avoid browsing to unknown sites on servers hosting Mitel products.

For software not provided by Mitel, Mitel recommends customers apply available security updates as they become available. Customers are advised to ensure operating system updates, including Windows, MacOS, iOS and Android, are applied to hosts and devices running Mitel software. Several vendors are providing guidance on potential performance impacts related to their security updates. Customers concerned about performance impacts are encouraged to review this vendor guidance.

Mitel continues to monitor for component updates and will be providing product updates. This advisory will be updated when Mitel product security updates are released.

External References

https://meltdownattack.com
https://www.us-cert.gov/ncas/current-activity/2018/01/03/Meltdown-and-Spectre-Side-Channel-Vulnerabilities

Related CVEs / CWEs / Advisories

CVE-2017-5715 (Branch target injection)
CVE-2017-5753 (Bounds check bypass)
CVE-2017-5754 (Rogue data cache load)

Revision History

Version	Date	Description
1.0	2018-01-08	Initial version