Side-Channel Analysis Method (Spectre and Meltdown)

Rev. 2.0
April 24, 2018
Fujitsu Limited

On January 3, 2018 a team of security researchers revealed new vulnerabilities that take advantage of techniques commonly used in many modern processor architectures. Collectively known as Meltdown and Spectre, these vulnerabilities utilize a new method of side-channel analysis and could allow an unprivileged attacker, in specific circumstances, to read privileged memory belonging to other processes or memory allocated to the operating system kernel. As a result, customers and prospects in different regions may raise concerns or seek advice and support from Fujitsu.

Below are the procedures to protect UNIX Servers.
For other Fujitsu products, please see CPU hardware vulnerable to side-channel attacks.

How to Protect UNIX Servers

- The UNIX Servers shown below are not affected by Meltdown (CVE-2017-5754) and Spectre Variant 2 (CVE-2017-5715).
- For Spectre Variant 1 (CVE-2017-5753), the minimum revisions of firmware and Oracle Solaris software releases to protect UNIX Servers are shown below. The firmware and Oracle Solaris SRU/patch can be applied in any order. Fujitsu's testing has shown that these fixes do not cause an impact on system performance.

  - Firmware for UNIX Servers

Product	Firmware with necessary updates
Fujitsu SPARC M12	XCP3051
Fujitsu M10	XCP2351
SPARC Enterprise M series	Firmware update is not needed

    XCP3051 and XCP2351 are available from your authorized service provider.

  - Oracle Solaris for UNIX Servers
    A specific Oracle Solaris 11 SRU is available from your authorized service provider.
    An Oracle Solaris 10 patch will be available at a later date from your authorized service provider.

Details

For more details, please see the following links.

- US-CERT: VU#584653: CPU hardware vulnerable to side-channel attacks
- CVE: CVE-2017-5715
- CVE: CVE-2017-5753
- CVE: CVE-2017-5754
- Intel Analysis of SpeculativeExecution Side Channels
- Intel Analysis of Speculative Execution Side Channels White Paper

Contact

For further information, please contact your authorized service provider.