Side-Channel Analysis Method

Rev. 6.0
January 31, 2022
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.
Variant 3a and Variant 4 are derivatives of side channel methods previously disclosed in January. Like the other variants, Variant 3a and Variant 4 use speculative execution, a feature common to most modern processor architectures, to potentially expose certain kinds of data through a side channel.

Below are the procedures to protect UNIX Servers. For other Fujitsu products, please see the following pages.

- CPU hardware vulnerable to side-channel attacks (CVE-2017-5715, CVE-2017-5753, CVE-2017-5754)
- CPU hardware vulnerable to side-channel attacks (CVE-2018-3639, CVE-2018-3640)

How to Protect UNIX Servers

- The UNIX Servers shown below are not affected by Meltdown (CVE-2017-5754), Spectre Variant 2 (CVE-2017-5715) and Spectre Variant 3a (CVE-2018-3640). In addition, SPARC M10 servers and SPARC Enterprise M series servers are not affected by Spectre Variant 1.1 (CVE-2018-3693), and SPARC Enterprise M series servers are not affected by Spectre Variant 1 (CVE-2017-5753) and Spectre Variant 4 (CVE-2018-3639).
- For Spectre Variant 1 (CVE-2017-5753) , Spectre Variant 1.1 (CVE-2018-3693) and Spectre Variant 4 (CVE-2018-3639), the minimum revisions of firmware and/or Oracle Solaris software releases to protect UNIX Servers are shown below. Fujitsu's testing with standard benchmark tools has shown that these fixes do not cause an impact on system performance.

- Spectre Variant 1 (CVE-2017-5753)

The firmware and Oracle Solaris SRU/patch can be applied in any order.

- ○ Firmware for UNIX Servers

Product	Firmware with necessary updates
Fujitsu SPARC M12	XCP 3051 or later
Fujitsu M10	XCP 2351 or later
SPARC Enterprise M series	Firmware update is not needed

XCP 3051 and XCP 2351 are available from your authorized service provider.

- ○ Oracle Solaris for UNIX Servers
  Specific Oracle Solaris 11 SRU/Oracle Solaris 10 patch are available from your authorized service provider.

- Spectre Variant 1.1 (CVE-2018-3693)

The following version of firmware must be applied.

- Firmware for UNIX Servers

Product	Firmware with necessary updates
Fujitsu SPARC M12	XCP 3090 or later
Fujitsu M10	Firmware update is not needed
SPARC Enterprise M series	Firmware update is not needed

XCP 3090 are available from your authorized service provider.

- Oracle Solaris for UNIX Servers

  No action is required.

- Spectre Variant 4 (CVE-2018-3639)

The following version of firmware must be applied.

- Firmware for UNIX Servers

Product	Firmware with necessary updates
Fujitsu SPARC M12	XCP 3052 or later
Fujitsu M10	XCP 2352 or later
SPARC Enterprise M series	Firmware update is not needed

XCP 3052 and XCP 2352 are available from your authorized service provider.

- Oracle Solaris for UNIX Servers

  No action is required.

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
- CVE: CVE-2018-3639
- CVE: CVE-2018-3640
- CVE: CVE-2018-3693
- US-CERT:
  - Alert (TA18-141A) Side-Channel Vulnerability Variants 3a and 4
  - VU#180049 CPU hardware utilizing speculative execution may be vulnerable to cache side-channel attacks

Contact

For further information, please contact your authorized service provider.