PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

23 March 2018
300402819 / imjl01

Security Advisory addressing Meltdown and Spectre vulnerabilities [CVE-2017-5754, CVE-2017-5715, CVE-2017-5753]

Synopsis

A bug in certain microprocessors may lead to information disclosure

Issue

Several CPUs manufactured by Intel, AMD or based on ARM technology may leak information due to their internal operation if attacked by specifically written software executed on the affected systems.
The information in this advisory is based on the statements of respective manufacturers.

Details

Microprocessors from Intel and AMD using the x86 architecture and some microprocessors using the ARM, PowerPC, and MIPS architecture may be susceptible to a group of attacks named Meltdown and Spectre. These attacks may lead to a (complete) disclosure of information in the memory of systems. Integrity and availability are not affected, but information gained using these weaknesses may be used in further attacks.
Meltdown [CVE-2017-5754] allows reading the complete memory of the attacked system using a specifically crafted executable code.
Spectre [version 1: CVE-2017-5753, version 2: CVE-2017-5715] allows reading the memory of other processes using a specifically crafted executable code or dynamic code as used in web browsers.

...

Only those systems can be affected that allow the installation/execution of custom code or load dynamic contents from foreign/untrusted sources. If only the root/administrative user can install/execute custom code, no additional risk exists, as the root/administrative user can read the information without exploiting this vulnerability. If a web browser can be used to view foreign web pages, the Spectre attack must be considered.

Systems that do not allow installation/execution of custom code are not affected.

Mitigation

On Industrial PCs and HMIs that operate with user installable or upgradable operating systems (mainly Windows) the latest version or update may be installed if required in the use case. As the update may have a performance impact, the application should be tested accordingly.

Affected products

The following control systems products are affected:

- AXC F 2152: Spectre v1/2; only “root/administrative user” can install custom code
- AXC 3051: Meltdown, Spectre v1/2; only “root/administrative user” can install custom code

The following embedded products are affected:

- FL MGUARD CENTERPORT: Meltdown, Spectre v1/2; only “root” can install custom code

The following HMI products are affected:

- TP 3000
- TP 3000/P
- TP 3000/WT
- TPM 3000
- WP 3000; only “root” can install custom code

The following Industrial PC products are affected:

- BL PPC 1000
- BL PPC12 1000
- BL PPC15 1000
- BL PPC17 1000
- BL BPC 2000
- BL BPC 2001
- BL BPC 3000
- BL BPC 3001
- BL PPC15 3000
- BL PPC17 3000
- BL BPC 7000
- BL BPC 7001
- BL PPC 7000

...

- BL PPC15 7000
- BL PPC17 7000
- BL RACKMOUNT 2U
- BL RACKMOUNT 4U
- BL2 BPC 1000
- BL2 PPC 1000
- BL2 BPC 2000
- BL2 PPC 2000
- BL2 BPC 7000
- BL2 PPC 7000
- DL PPC15 1000
- DL PPC15M 7000
- DL PPC18.5M 7000
- DL PPC21.5M 7000
- EL PPC 1000
- EL PPC 1000/WT
- EL PPC 1000/M
- VALUELINE IPC
- VL BPC 1000
- VL BPC 2000
- VL PPC 2000
- VL BPC 3000
- VL PPC 3000
- VL IPC P7000
- VL2 BPC 1000
- VL2 PPC 1000
- VL2 BPC 2000
- VL2 PPC 2000
- VL2 BPC 3000
- VL2 PPC 3000
- VL2 BPC 7000
- VL2 PPC 7000
- VL2 BPC 9000
- VL2 PPC 9000
- VL2 PPC7 1000
- VL2 PPC9 1000
- VL2 PPC12 1000