CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Security Advisory for Meltdown and Spectre Attacks in HMI Devices

Document ID TDOCT-6012_ENG
Publication date 2018-02-09

Vulnerabilities or CVE Identifier

CVE-2017-5753, CVE-2017-5715, CVE-2017-5754

Severity

5.6 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

Affected products

VisuNet RM*, VisuNet PC*, Box Thin Client BTC*
(All products within these families)

Vulnerability Type

Information Disclosure

Summary

Critical vulnerabilities within several CPUs have been identified by security researchers. These hardware vulnerabilities allow programs to learn about the contents of a system's memory, using side-channel attacks. Potential attack vectors against these vulnerabilities have been published and dubbed Meltdown and Spectre. While programs are typically not permitted to read data from the OS kernel or from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in kernel memory or the memory of other programs executed on the same CPU. As a consequence, an exploit could allow attackers to get access to any sensitive data, including passwords or cryptographic keys.

Impact

Pepperl+Fuchs analyzed HMI devices in respect of Meltdown and Spectre attacks. To our current knowledge only VisuNet HMI devices and Box Thin Clients, based on an Intel® CPU, are potentially affected by these vulnerabilities.

In order to exploit these vulnerabilities, an attacker needs to be able to execute arbitrary code on the CPU of the target system.

Since Pepperl+Fuchs HMI devices are designed and usually used in Industrial Control System (ICS) networks, typically ICS networks are segregated from enterprise networks and do not have direct internet access. Additionally, VisuNet HMI devices use a kiosk mode for normal operation. Within this mode access policies of thin client based VisuNet Remote Monitors and Box Thin Clients are restricted, such that users can only access predefined servers. This implies that outgoing connections and local software installations have to be configured by administrators. Hence, operators are restricted in a way such that they can only use the system as configured by administrators. If these steps are taken, this greatly reduces the risk of unwittingly accessing malicious content and executing unknown code, e.g. by accessing a website that was prepared by an attacker.

However, if a malicious website is accessed, an attacker could gain knowledge of all data in the memory of the HMI device, including passwords.

Solution

Customers using HMI devices out of VisuNet RM*, VisuNet PC* or Box Thin Client BTC* product families should follow these guidelines:

- Pepperl+Fuchs HMI devices should be segregated from enterprise networks and internet.
- Preconfigured server connections / websites should be restricted to secured and trusted servers. The use of secure protocols, e.g. HTTPS, is recommended.
- In case websites are configured in kiosk mode, it should be ensured that whitelisted websites do not redirect to untrusted servers / websites.
- For VisuNet RM* and Box Thin Client with Shell 4.x an update 18-33537 LINK which includes Windows security patches published by Microsoft is available on the Pepperl+Fuchs website.
- For VisuNet PC* systems with Microsoft Windows Operating Systems, Microsoft offers security patches which can be directly downloaded from the Microsoft website.

Please note that Microsoft Security patches directly affect machine code execution on the CPU. Be aware of installing these patches, because they might have an impact on system performance or system stability.
This advisory will be updated as further details and/or software updates become available.

Reported by

Jann Horn (Google Project Zero), Werner Haas, Thomas Prescher (Cyberus Technology), Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology) published the attack on **https://meltdownattack.com/**

Jann Horn (Google Project Zero) and Paul Kocher, Daniel Genkin (University of Pennsylvania and University of Maryland), Mike Hamburg (Rambus), Moritz Lipp (Graz University of Technology), and Yuval Yarom (University of Adelaide and Data61) published the attack on **https://meltdownattack.com/**

Support

For support please contact your local Pepperl+Fuchs sales representative.