WOODWARD

Cyber Security Bulletin
(2018-04_1 Rev -)

Meltdown/Spectre Exploit

Issue

The early January, ICS-CERT released information disclosed in December on two side-channel exploits, Meltdown and Spectre. Meltdown affects Intel based chips, however Spectre impacts additional chips such as ARM, AMD and NXP. Spectre affects a variety of operating systems and chips and relies on “Speculative Execution”.

Description

The following information is from CERT: CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre. Both Spectre and Meltdown take advantage of the ability to extract information from instructions that have executed on a CPU using the CPU cache as a side channel. These attacks are described in detail by Google Project Zero, the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz) and Anders Fogh. The issues are organized into three variants:

- Variant 1 (CVE-2017-5753, Spectre): Bounds check bypass
- Variant 2 (CVE-2017-5715, also Spectre): Branch target injection
- Variant 3 (CVE-2017-5754, Meltdown): Rogue data cache load, memory access permission check performed after kernel memory read

An attacker able to execute code with user privileges can achieve various impacts. The Meltdown attack allows reading of kernel memory from user space. This can result in privilege escalation, disclosure of sensitive information, or it can weaken kernel-level protections, such as KASLR. The Spectre attack can allow inter-process or intra-process data leaks.

To execute code locally, an attacker would require a valid account or independent compromise of the target. Attacks using JavaScript in web browsers are possible. Multi-user and multi-tenant Windows systems (including virtualized and cloud environments) likely face the greatest risk. Systems used to browse arbitrary web sites are also at risk. Single-user systems that do not readily provide a way for attackers to execute code locally face/have significantly lower risk.

Affected Units

Customers using Microsoft Windows operating systems, specifically the SOS application. Legacy Pentium/NT, MicroNet™, and Atlas PC have low risk – see below.

HMI systems and engineering workstations that may be attached to a Woodward control system utilize Microsoft Windows and are potentially impacted. See notes under “Corrective Actions.”

Woodward controls (MicroNet, MicroNet+, Atlas, 505), with the exception of the NT CPU and the Atlas PC are not impacted by Meltdown or Spectre.

Users have reported issues with SOS on Windows systems patched by KB4056892. You can view Windows Update history by viewing Control Panel\System and Security\Windows Update\View Update History. It is recommended to avoid installing this knowledge base update. Microsoft has released a new patch KB4088776 to address this issue.

Impact to MicroNet Simplex NT CPU and Atlas PC (NT version) with Pentium CPUs:

Web browsing and JavaScript hosting is not available on the NT CPU and Atlas PC controls. Local code execution will require physical access to the control and upload of an unauthorized executable to the control to exploit. Since this is a side-channel exploit, data can only be observed, and not directly manipulated.

Note: Woodward's current industrial control products (including MicroNet Plus, MicroNet TMR, Atlas II, 505 and Flex500) are not directly impacted by Meltdown or Spectre.

Corrective Action

Windows-based HMI and Engineering Workstation Computers:

Woodward normally recommends that the end-user's IT department or other group responsible for maintaining these computers keep these machines updated with the latest Microsoft security patches. However, in the case of Spectre and Meltdown, there have been significant issues with the Windows patches issued by Microsoft. You can view Windows Update history by viewing Control Panel\System and Security\Windows Update\View Update History.

Please see notes below regarding recommendations on specific patches:

- Users have reported issues with SOS on Windows systems patched by KB4056892. Recommend not installing this knowledge base update. Microsoft has released a new patch KB4088776 to address this issue.
- If the user has installed KB4056892 and SOS exhibits issues, the user should uninstall KB4056892. If the user is unable to uninstall this update or uninstall does not address the issue, DCOM configuration in Windows may need to be changed.
- KB4088776 addresses issues created by KB4056892 regarding DCOM and OPC (thus impacting SOS server functionality)

MicroNet Simplex and Atlas PC systems with Pentium CPU:

Implement physical security so that unauthorized code updates cannot be made.

Customer Action

Review the Corrective Action above for impact on your specific industrial control system and review Additional Information below.

Additional Information

A side-channel exploit/attack is any attack based on information gained from the implementation of a computer system, rather than a weakness in the computer system

ICS-CERT Alert (18-011-01FB) - https://ics-cert.us-cert.gov/alerts/ICS-ALERT-18-011-01F

CERT Vulnerability Note (VU#584653) - https://www.kb.cert.org/vuls/id/584653

OPC Foundation Meltdown/Spectre patch - https://opcfoundation.org/news/opc-foundation-news/meltdown-spectre-patch/

WOODWARD

PO Box 1519, Fort Collins CO 80522-1519, USA
1041 Woodward Way, Fort Collins CO 80524, USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.