Cyber Advisory: Meltdown & Spectre

KB0025590

Meltdown & Spectre

Introduction

Information security researchers have found two major security vulnerabilities, dubbed "Meltdown" and "Spectre," that affect the processing chips in almost every computer made in the last 20 years (including mobile phones, embedded devices, cloud computers, etc.).

Meltdown and Spectre

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware bugs allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Risk due to Vulnerability

Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.

Spectre breaks the isolation between different applications. It allows an attacker to trick error free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre.

Risk Management

GE Power Cybersecurity and Engineering teams believe the Meltdown and Spectre vulnerability risk is low, but not negligible.

At GE (M&D), we have implemented a good defense-in-depth strategy to minimize the risk that vulnerabilities like Meltdown/Spectre represent to the OSM. Some of our controls include:

- Implementation of a standard Network Architecture for OSM operation that is based on a security zone model that segments the network into zones. A "trusted-zone" is created within the customer environment to segment the controllers from non-trusted environments where the OSM reside
- A firewall is installed to serve as the Network Control Point (NCP) that protects and controls data traffic to this security zone
- OSM servers are not internet facing
- A VPN dedicated to OSM access is used to reach the OSM server from M&D
- GE M&D Support Engineers connect to a jump host using remote desktop technology to access the OSM server

- All inbound and outbound communications are examined to detect malicious communication
- OSM servers are regularly patched
- M&D has developed and implemented a proper and mature vulnerability management process that covers all components including servers, network components, software library, firmware, etc

GE recommends adopting a cyber security risk management program which includes proactive assessment based on the plant's inventory of control system network components. This includes monitoring and planning for near and long-term actions to protect your system from component EoL and cyber risks.

Suggested actions include basic inspection of control component version for both hardware and software, including patching status and OEM EoL plans for component lifecycle. This status needs to be evaluated against your corporate governance and risk tolerance.

Due to the variation in customer networks, GE cannot validate all firmware and software patch updates released by manufacturers. The following is generally recommended if users decide to apply patches.

1. Take an image backup of the device to be updated (HMI, historian, etc.)
2. Update the antivirus definitions/software.
3. Run and install the applicable software update/patch. In rare instances, updates/patches may impact the device's function. As such, new updates should be tested within a testbed platform before installing into a production environment, if a testbed is not feasible, apply update to only one or two devices before being propagated to the entire plant.

For more information on the Meltdown and Spectre vulnerabilities, please refer to the following links.

https://meltdownattack.com/

https://youtu.be/syAdX44pokE

Meltdown: https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-5754

Spectre: https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-5753

https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-5715

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0025590