protiviti®
Face the Future with Confidence

Security Advisory – New Class of Vulnerabilities Introduced to Enterprise Systems: Meltdown and Spectre

January 8,
2018

Description of the Vulnerability

For the first time, a performance-enhancing feature of most modern processors (known as speculative execution and branch prediction) was discovered to contain a flaw that allows unauthorized disclosure of information. The fact that this flaw is at the processor level differentiates it from other potential vulnerabilities in terms of the number and variety of systems impacted.

Security researchers have demonstrated an attack in most major processor manufacturers, including Intel, AMD and ARM. The vulnerabilities could be exploited in servers, end user workstations (including laptops), network infrastructure, mobile devices, IoT devices and consumer electronics – essentially any system utilizing an impacted processor.

The MITRE Corporation[1] has released three distinct Common Vulnerabilities and Exposures (CVEs), the standard for information security vulnerability names, which are as follows:

- **Spectre**: CVE-2017-5753 and CVE-2017-5715
- **Meltdown**: CVE-2017-5754

These vulnerabilities allow an authenticated attacker with access to a company's system to execute code that may compromise data currently being processed on the system within other processes. This means the attacker must have physical or logical access of the system to exploit, or has exploited a separate vulnerability to be able to take advantage of these processor level vulnerabilities remotely. Memory (data) controlled by one process is not typically able to be accessed by another process. These vulnerabilities circumvent current

[1] The MITRE Corporation manages federally funded research and development centers supporting several U.S. government agencies, including the National Cyber Security Division of the United States Department of Homeland Security. MITRE manages the Common Vulnerabilities and Exposures (CVE) system, which provides an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.

protections and currently have publically available exploit code. Detailed information can be found at: https://meltdownattack.com/

This exposure means that passwords, documents, emails and other data residing on affected systems may be at risk. In a shared services environment, such as many cloud environments, there is the risk of one customer using the attack to access data of another customer being processed on the same hardware.

Wait, the Cloud? What Should an Organization that Uses the Cloud Do?

Thankfully, the researchers who identified these vulnerabilities followed responsible disclosure practices, and mitigations are already widely available for various platforms. Each of the three major cloud hosting providers have provided responses to these vulnerabilities.

- **Amazon Web Services (AWS) –** AWS indicates that all instances across the EC2 fleet have been protected, and AWS recommends that users patch their operating system instances as well. For more from AWS, read their bulletin here: https://aws.amazon.com/security/security-bulletins/AWS-2018-013/
- **Google Cloud Platform** – Google reports that their Google Cloud Platform (GCP) and G Suite environments have been fully patched against these vulnerabilities, and they recommend that users patch any operating systems they use within GCP. For more information, read their bulletin here: https://blog.google/topics/google-cloud/what-google-cloud-g-suite-and-chrome-customers-need-know-about-industry-wide-cpu-vulnerability/
- **Microsoft Azure** – According to Microsoft, the Azure infrastructure has been updated, and if deemed necessary, vulnerable VM instances were forcibly rebooted. Microsoft also recommends that security best practices be followed for all VMs. For more information, read Microsoft's bulletin here: https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/

What Should Organizations Do?

Organizations should immediately move to evaluate impacted systems and address any issues as part of their vulnerability and patch management program. From that point, the actions required are not substantially different from a response to a normal vulnerability requiring a software update:

- Patch, but don't be careless. The vulnerabilities require that an attacker has already obtained access to the target system, so put the patches through the standard patch

processes that include testing. Ensure that proper testing is performed to identify potential adverse system performance or issues. Microsoft has already discovered that the Windows patches that remedy this issue created issues with a small number of AntiVirus products. Up-to-date information can be found here: https://support.microsoft.com/en-hk/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software

- Monitor the performance impact on critical applications, services and workloads, paying specific attention to those with a history of performance or capacity issues. Initial analysis suggests that the patches for these vulnerabilities have been shown to cause a performance impact. Incorporate these results into decisions related to the application of the patches in production and the potential need to adjust the entity's systems architecture for data processing.

- Use the organization's third party risk assessment program or other established processes to reach out to partners that process sensitive data and solicit information as to how they are responding to these vulnerabilities.

- Be aware of the variety of systems impacted. Patch management programs that focus on the end user environment and specific server platforms, such as Windows or Linux, will not have sufficient coverage to manage this risk. Work to identify and address other impacted systems within the environment. Impacted systems that may "slip through the cracks" include virtualized platforms and systems, connected devices, and vendor systems that are sitting on the company network.

- Be prepared to give updates on the status of the issue. With the visibility on the action, company leadership and possibly the board of directors may request updates on status. Provide transparent updates that give an appropriate sense of the risk exposure, actions being taken to mitigate the risk and any potential impact on the business that may occur.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®