ANJOLEN
Securing Your Cyber Future

Important Cybersecurity Update

Meltdown and Spectre Processor Security Flaws

Vulnerability Description

Meltdown and Spectre are vulnerabilities that are caused due to a design flaw in computer processor chipsets made by Intel, AMD and ARM. The vulnerability is caused by the chip's attempt to read data ahead and execute out of order operations.

Systems Affected

These vulnerabilities affect almost all modern systems manufactured in the past 20 years, including desktops, laptops, cellular phones and Internet of things devices.

Risks

Meltdown and Spectre are both capable of accessing data within active memory which could include passwords and other sensitive information. Neither vulnerability is known to be capable of accessing stored data such as information saved to a hard drive. Neither Meltdown nor Spectre is known to have been utilized in an active attack in the wild.

Protection

Anti-virus and anti-malware applications are not likely to be capable of identifying attacks related to these vulnerabilities. At their core, both Meltdown and Spectre are caused by hardware design flaws, however, software fixes can mitigate their impact.

Recommended Steps

1. Eliminate the use of any out of date or legacy Internet browsing software. Update all current browsers to the latest version.
2. Identify operating system patches related to Meltdown and Spectre and apply as soon as possible.
3. Check for motherboard and chipset firmware updates and apply as available
4. Continue to monitor security bulletins related to Spectre and Meltdown in order to identify the most current mitigation efforts.

Conclusion

Meltdown and Spectre are vulnerabilities caused by a design flaw in almost all modern computer processors made by all of the major chipset manufacturers. Affected devices include most desktop, laptop and cellular telephones manufactured in the past 20 years. These vulnerabilities are not known to have been actively employed in an attack in the wild yet, but are theoretically capable of stealing memory resident data that could include passwords and other sensitive information. Data storage devices such as hard drives are not affected by these vulnerabilities. Patches and updates, particularly for Internet browsers can mitigate some of the potential attack vectors of Meltdown and Spectre and should be applied as soon as possible.

Need help implementing these recommendations? Call us and ask about our VCISO services to help you implement the recommended steps. Already have a VCISO contract with us? Call us to use your hours toward these recommended steps.