CERT/CC Vulnerability Note VU#155143

4-6 minutes

Overview

A new cross-privilege Spectre v2 vulnerability that impacts modern CPU architectures supporting speculative execution has been discovered. CPU hardware utilizing speculative execution that are vulnerable to Spectre v2 branch history injection (BHI) are likely affected. An unauthenticated attacker can exploit this vulnerability to leak privileged memory from the CPU by speculatively jumping to a chosen gadget. Current research shows that existing mitigation techniques of disabling privileged eBPF and enabling (Fine)IBT are insufficient in stopping BHI exploitation against the kernel/hypervisor.

Description

Speculative execution is an optimization technique in which a computer system performs some task preemptively to improve performance and provide additional concurrency as and when extra resources are available. However, these speculative executions leave traces of memory accesses or computations in the CPU's cache, buffer, and branch predictors. Attackers can take advantage of these and, in some cases, also influence speculative execution paths via malicious software to infer privileged data that is part of a distinct execution. See article Spectre Side Channels for more information. Attackers exploiting Spectre v2 take advantage of the speculative execution of indirect branch predictors, which are steered to gadget code by poisoning the branch target buffer of a CPU used for predicting indirect branch addresses, leaking arbitrary kernel memory and bypassing all currently deployed mitigations.

Current mitigations rely on the unavailability of exploitable gadgets to eliminate the attack surface. However, researchers demonstrated that with the use of their gadget analysis tool, InSpectre Gadget, they can uncover new, exploitable gadgets in the Linux kernel and that those are sufficient at bypassing deployed Intel mitigations.

Impact

An attacker with access to CPU resources may be able to read arbitrary privileged data or system registry values by speculatively jumping to a chosen gadget.

Solution

Please update your software according to the recommendations from respective vendors with the latest mitigations available to address this vulnerability and its variants.

Acknowledgements

Thanks to Sander Wiebing, Alvise de Faveri Tron, Herbert Bos, and Cristiano Giuffrida from the VUSec group at VU Amsterdam for discovering and reporting this vulnerability, as well as supporting coordinated disclosure. This document was written by Dr. Elke Drennan, CISSP.

Vendor Information

Filter by content: Additional information available

Sort by:

References

- https://www.intel.com/content/www/us/en/developer/topic-technology/software-security-guidance/processors-affected-consolidated-product-cpu-model.html
- https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/advisory-guidance/branch-history-injection.html
- https://www.vusec.net/projects/bhi-spectre-bhb/
- https://vuls.cert.org/confluence/display/Wiki/Vulnerabilities+Associated+with+CPU+Speculative+Execution
- https://www.commerce.senate.gov/2018/7/complex-cybersecurity-vulnerabilities-lessons-learned-from-spectre-and-meltdown
- https://www.economist.com/business/2018/01/11/spectre-and-meltdown-prompt-tech-industry-soul-searching

Other Information

CVE IDs:	CVE-2022-0001 CVE-2024-2201
API URL:	VINCE JSON | CSAF
Date Public:	2024-04-09
Date First Published:	2024-04-09
Date Last Updated:	2024-12-19 20:29 UTC
Document Revision:	9