



SIDE CHANNEL ANALYSIS SECURITY ISSUE

3 2018

BRIEFING OBJECTIVES

- Provide information on a new class of security issue & mitigation
- Provide context on how this issue has brought the industry together

BACKGROUND & SUMMARY

Security researcher notified Intel, AMD, and ARM of a new side-channel analysis exploit

- A method for an attacker to observe contents of privileged memory, circumventing expected privilege levels
- Exploits *speculative execution* techniques common in modern processors
- NOT unique to any one architecture or processor implementation
- NOT a result of product errata; processors are operating to specification
- Mitigations include updates to system software, firmware and future hardware

INDUSTRY-WIDE COLLABORATION TO FACILITATE RESPONSIBLE DISCLOSURE WITH MITIGATION OPTIONS

WHAT IT IS, WHAT IT IS NOT

IS

- A method for an attacker to observe contents of privileged memory, circumventing expected privilege levels
- Malware using this method and running *locally* could expose sensitive data such as passwords and encryption keys

IS NOT

- A denial of service attack
- A network attack
- A means to inject malicious code or corrupt memory

WE HAVE NOT OBSERVED ACTIVE DEPLOYMENT OF THIS EXPLOIT

OUR APPROACH TO MITIGATION

We are taking a comprehensive approach to provide the most secure platforms

Combination of operating system and firmware updates, developed in collaboration with industry partners, operating system vendors, and OEMs

Expect mitigation will be available to users beginning over the next few days and continuing over several weeks

SECURITY ISSUE VARIANTS

Summary	Description	Mitigation Options
Bounds Check Bypass	Use existing code with access to secrets by making it speculatively execute memory operations	OS & VMM updates
Branch Target Injection	Malicious code usurps properties of CPU branch prediction features to speculatively run code	OS & VMM updates Firmware Updates
Rogue Data Load	Access memory controlled by the OS while running a malicious application.	OS updates

ALL VARIANTS ARE LOCALLY EXECUTED SIDE-CHANNEL CACHE TIMING ATTACKS

Q & A

Risk Factors

This presentation occurs during Intel's "Quiet Period," before Intel announces its financial and operating results for the fourth quarter of 2017. Therefore, presenters will not be addressing fourth quarter results during this presentation. Statements in this presentation that refer to forecasts, future plans and expectations are forward-looking statements that involve a number of risks and uncertainties. Words such as "anticipates," "expects," "intends," "goals," "plans," "believes," "seeks," "estimates," "continues," "may," "will," "would," "should," "could," and variations of such words and similar expressions are intended to identify such forward-looking statements. Statements that refer to or are based on projections, uncertain events or assumptions also identify forward-looking statements. Such statements are based on management's current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in these forward-looking statements. Important factors that could cause actual results to differ materially from the company's expectations are set in Intel's earnings release dated October 26, 2017, which is included as an exhibit to Intel's Form 8-K furnished to the SEC on such date. Additional information regarding these and other factors that could affect Intel's results is included in Intel's SEC filings, including the company's most recent reports on Forms 10-K and 10-Q. Copies of Intel's Form 10-K, 10-Q and 8-K reports may be obtained by visiting our Investor Relations website at www.intc.com or the SEC's website at www.sec.gov.