Security Newsletter

20 August 2018

Subscribe to this newsletter

Intel Has a New Speculative Execution Issue: Foreshadow

The Meltdown and Spectre vulnerabilities revealed earlier this year showed how the quest to make CPUs run faster inadvertently introduced serious security vulnerabilities that could be used to access sensitive data. Now, researchers have unveiled a new attack called Foreshadow that builds on those speculative execution flaws, affecting millions of Intel processors made over the past five years. It's particularly dangerous because Foreshadow can be triggered from the user space and does not require a privileged attacker with root access.

The vulnerability has been kept under wraps since January as Intel has developed mitigations. Intel also found two variants of the Foreshadow attack, one of which could affect cloud-computing environments. While Foreshadow is serious, Intel says it expects its impact on consumers and enterprises in non-virtualized environments to be low. The chip manufacturer has issued microcode fixes all three variations of the vulnerability, two of which it believes have been sufficiently mitigated.

Intel, operating system and hypervisor vendors have issued update to mitigate the CVE-2018-3646 aspect of Foreshadow, but Intel says in some cases, more defensive steps may need to be taken.

Read More

Even More

Cutting room floor

- Faxploit: Hackers can use Fax machines to inject malware into a targeted network
- Popular Android Apps Vulnerable to Man-in-the-Disk Attacks
- ex-NSA Hacker Discloses macOS High Sierra Zero-Day Vulnerability
- VORACLE Attack Can Recover HTTP Data From VPN Connections
- Skim Reaper Device That Detects Wide Range of Skimmer Devices
- Microsoft Patch Tuesday: 60 vulnerabilities resolved including two active exploits
- Email Phishers Using New Way to Bypass Microsoft Office 365 Protections
- Melbourne teen hacked into Apple's secure computer network, court told
- 2018 Pwnie Awards: Winners are up
- Two DDoS Friendly Bugs Fixed in Linux Kernel
- Chrome Bug Allowed Hackers to Find Out Everything Facebook Knows About You
- Btlejacking Attack Could Allow a Hacker to Jam and Takeover the Bluetooth Connection
- New PHP Code Execution Attack Puts WordPress Sites at Risk
- Mozilla wipes 23 Firefox add-ons off the map for tracking user activity
- Commercial Cryptographic Key Management in 2018

#Tech and #Tools

- Reliable, Secure and Universal Backup for U2F Token
- The pfSense book
- ReportingObserver: know your code health
- OpenSSH Username Enumeration through malformed packets
- Welcome to the New Order: A DEF CON 2018 CTF Retrospective
- Commercial Cryptographic Key Management in 2018
- L1 Terminal Fault / CVE-2018-3615 , CVE-2018-3620,CVE-2018-3646 / INTEL-SA-00161
- Generates gopher link for exploiting SSRF and gaining RCE in various servers
- CVE-2018-8340: Multi-Factor Mixup in Microsoft ADFS
- The Dangers of Key Reuse: Practical Attacks on IPsec IKE
- Evading Anomaly-Based NIDS with Empire
- Password and Credential Management in 2018
- Acra: Database encryption proxy for data-driven apps: strong selective encryption, SQL injections prevention, intrusion detection, honeypots.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us