Out-Law.com
Legal news and guidance from Pinsent Masons

Topics
- >
TMT & Sourcing
- >
Cybersecurity

Security flaws found in 'most' modern computer processors

Security flaws have been identified in the way many computer processors operate, according to security researchers at Google.05 Jan 2018

- Cybersecurity
- TMT & Sourcing
- TMT
- Advanced Manufacturing & Technology
- UAE
- UK
- China
- Southern Africa
- Europe
- Germany
- Qatar
- Eastern Africa
- Asia Pacific
- North Africa
- Central Asia
- France
- Middle East
- Africa
- South east Asia
- Western Africa
- Australia

Matt Linton, a senior security engineer at Google, and colleague Pat Parseghian, technical program manager, said the company had decided to go public about the problem prior to a planned "coordinated disclosure date" of 9 January following reports of the issue in the media.

The Register reported on the existence of the 'Meltdown' and 'Spectre' flaws on Wednesday.

In a blog, Linton and Parseghian said that the "serious security flaws" had been identified by security researchers in Google's 'Project Zero' team last year. The vulnerabilities arise from a method "most modern processors" deploy to "optimise performance", they said.

"The Project Zero researchers discovered three methods (variants) of attack, which are effective under different conditions," according to the blog. "All three attack variants can allow a process with normal user privileges to perform unauthorised reads of memory data, which may contain sensitive information such as passwords, cryptographic key material, etc."

"In order to improve performance, many CPUs may choose to speculatively execute instructions based on assumptions that are considered likely to be true. During speculative execution, the processor is verifying these assumptions; if they are valid, then the execution continues. If they are invalid, then the execution is unwound, and the correct execution path can be started based on the actual conditions. It is possible for this speculative execution to have side effects which are not restored when the CPU state is unwound, and can lead to information disclosure," it said.

"There is no single fix for all three attack variants; each requires protection independently. Many vendors have patches available for one or more of these attacks," it said.

Processor giant Intel, one of the companies whose products are potentially exposed by the flaws, said it is "working closely with many other technology companies, including AMD, ARM Holdings and several operating system vendors, to develop an industry-wide approach to resolve this issue promptly and constructively".

In a statement, Intel said it has "begun providing software and firmware updates to mitigate these exploits".

“Check with your operating system vendor or system manufacturer and apply any available updates as soon as they are available," Intel said. "Following good security practices that protect against malware in general will also help protect against possible exploitation until updates can be applied."

“Intel believes its products are the most secure in the world and that, with the support of its partners, the current solutions to this issue provide the best possible security for its customers," it said.

More from Out-Law.com

- Regulator reports growing concern from EU banks about cyber risk and data security 28 Nov 2017
- Firms advised to assess their suppliers' cyber resilience in the same way they do their own 20 Nov 2017
- Cyber breach response should involve organising and prioritising several workstreams through a central incident response team, says expert 20 Nov 2017

Related Sectors

- TMT
- Advanced Manufacturing & Technology

All sectors

Latest Cybersecurity News & Guides

- PSD2: no cross-checking on consent needed, says EBA 15 Jun 2018
- Service level standards set to be stipulated for UK banks 15 Jun 2018

- Prosecutions for white collar crime continue to fall 12 Jun 2018
- Guide: The Network and Information Security Directive – implications for the energy sector
- Guide: Cryptography

Join My Out-Law

- **See only the content that matters to you**
- **Tailor Out-Law to your exact needs**
- **Save the most useful content for later reading**
- **Tailor our weekly eNewsletter to your interests**

Join My Out-Law

Already signed up to My Out-Law?

Sign in

Pinsent Masons

Expertise in TMT & Sourcing

Pinsent Masons provides strategic and contractual advice to organisations across the public and private sectors.

More about TMT & Sourcing

-

Marc Dautlich
Partner - Head of Information Law

View profile

More about Pinsent Masons

© Copyright Pinsent Masons LLP