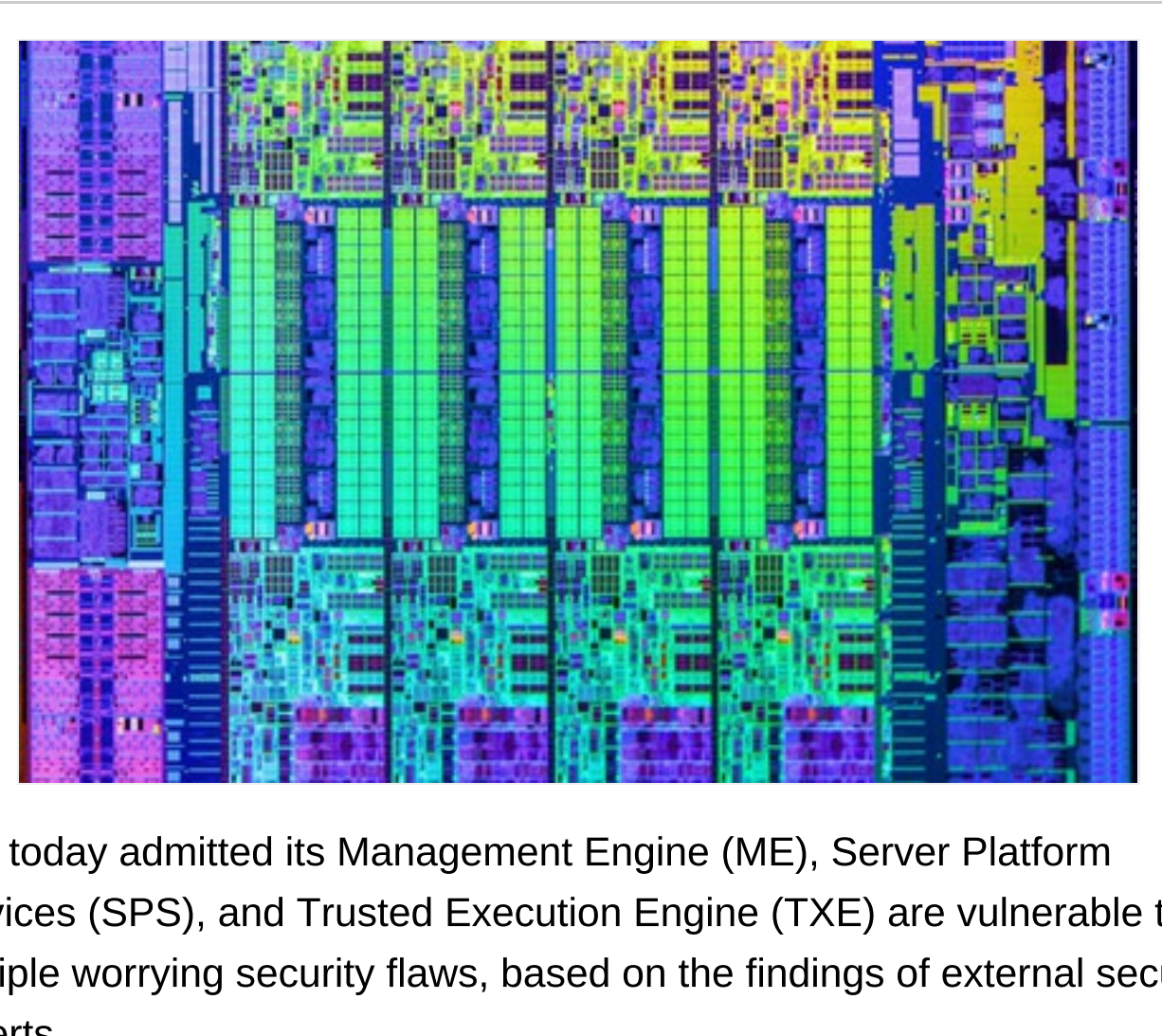
heise online The Register — WannaCry: Wenn die Malware von heute der KI von gestern nicht gewachsen ist

Security

Intel finds critical holes in secret Management Engine hidden in tons of desktop, server chipsets

Bugs can be exploited to extract info, potentially insert rootkits

By Thomas Claburn in San Francisco 20 Nov 2017 at 23:53 79 SHARE ▼



Intel today admitted its Management Engine (ME), Server Platform Services (SPS), and Trusted Execution Engine (TXE) are vulnerable to multiple worrying security flaws, based on the findings of external security experts.

The firmware-level bugs allow logged-in administrators, and malicious or hijacked high-privilege processes, to run code beneath the operating system to spy on or meddle with the computer completely out of sight of other users and admins. The holes can also be exploited by network administrators, or people masquerading as admins, to remotely infect machines with spyware and invisible rootkits, potentially.

Meanwhile, logged-in users, or malicious or commandeered applications, can leverage the security weaknesses to extract confidential and protected information from the computer's memory, potentially giving miscreants sensitive data – such as passwords or cryptographic keys – to kick off other attacks. This is especially bad news on servers and other shared machines.

In short, a huge amount of Intel silicon is secretly running code that is buggy and exploitable by attackers and malware to fully and silently compromise computers. The processor chipsets affected by the flaws are as follows:

- 6th, 7th and 8th Generation Intel Core processors
- Intel Xeon E3-1200 v5 and v6 processors
- Intel Xeon Scalable processors
- Intel Xeon W processors
- Intel Atom C3000 processors
- Apollo Lake Intel Atom E3900 series
- Apollo Lake Intel Pentiums
- Celeron N and J series processors

Intel's Management Engine, at the heart of today's disclosures, is a computer within your computer. It is Chipzilla's much maligned coprocessor at the center of its vPro suite of features, and it is present in various chip families. It has been assailed as a "backdoor" – a term Intel emphatically rejects – and it is a mechanism targeted by researchers at UK-based Positive Technologies, who are set to reveal in detail new ways to exploit the ME next month.

The Management Engine is a barely documented black box. it has its own CPU and its own operating system – recently, an x86 Quark core and MINIX – that has complete control over the machine, and it functions below and out of sight of the installed operating system and any hypervisors or antivirus tools present.

It is designed to allow network administrators to remotely or locally log into a server or workstation, and fix up any errors, reinstall the OS, take over the desktop, and so on, which is handy if the box is so messed up it can't even boot properly.

The ME runs closed-source remote-administration software to do this, and this code contains bugs – like all programs – except these bugs allow hackers to wield incredible power over a machine. The ME can be potentially abused to install rootkits and other forms of spyware that silently snoop on users, steal information, or tamper with files.

SPS is based on ME, and allows you to remotely configure Intel-powered servers over the network. TXE is Intel's hardware authenticity technology. Previously, the AMT suite of tools, again running on ME, could be bypassed with an empty credential string.

Today, Intel has gone public with more issues in its firmware. It revealed it "has identified several security vulnerabilities that could potentially place impacted platforms at risk" following an audit of its internal source code:

> **In response to issues identified by external researchers, Intel has performed an in-depth comprehensive security review of our Intel Management Engine (ME), Intel Server Platform Services (SPS), and Intel Trusted Execution Engine (TXE) with the objective of enhancing firmware resilience.**

The flaws, according to Intel, could allow an attacker to impersonate the ME, SPS or TXE mechanisms, thereby invalidating local security features; "load and execute arbitrary code outside the visibility of the user and operating system"; and crash affected systems. The severity of the vulnerabilities is mitigated by the fact that most of them require local access, either as an administrator or less privileged user; the rest require you to access the management features as an authenticated sysadmin.

Intel ME controller chip has secret kill switch

READ MORE →

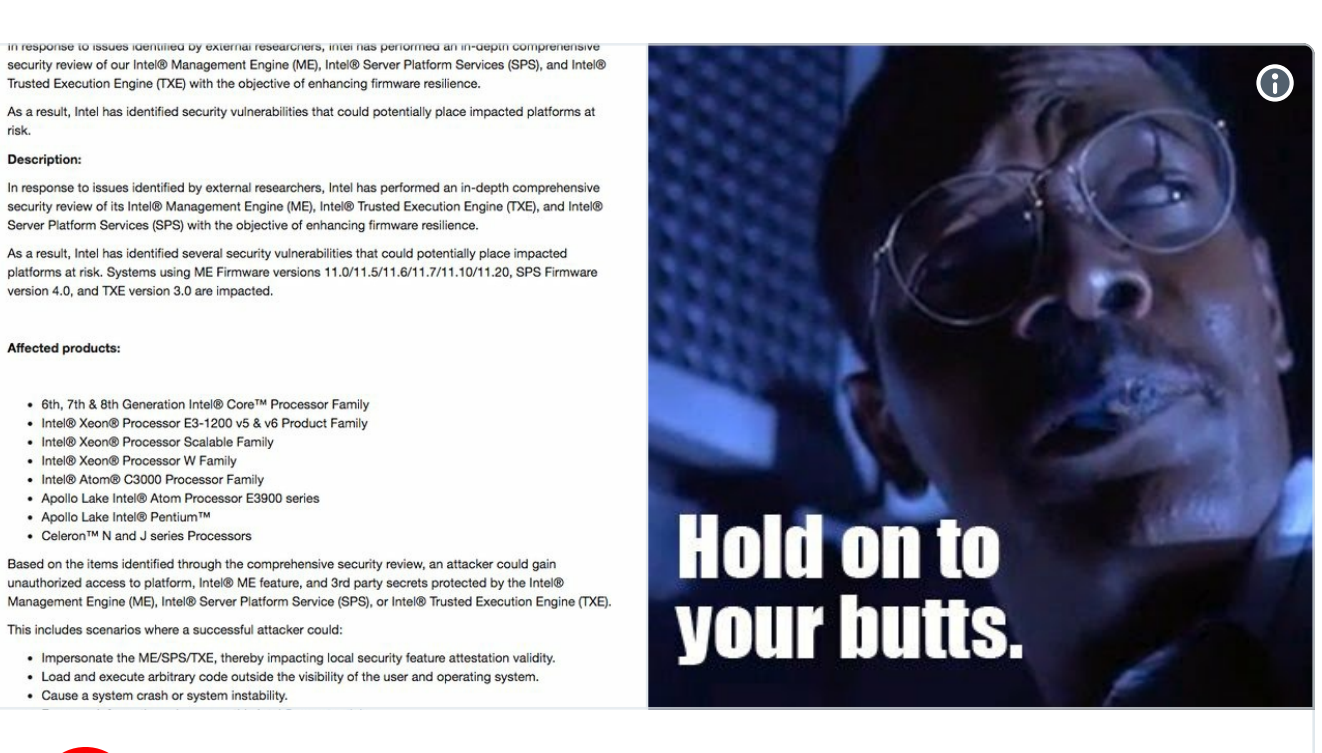
But as Google security researcher Matthew Garrett pointed out in the past hour or so, the aforementioned AMT flaw, if not patched, could allow remote exploitation.

In other words, if a server or other system with the AMT hole hasn't been updated to kill off that vulnerabilities, these newly disclosed holes will allow anyone on the network to potentially log in and execute malicious code within the powerful ME coprocessor.

"The ME compromise presumably gives you everything the AMT compromise gives you, plus more," said Garrett via Twitter. "If you compromise the ME kernel, you compromise everything on the ME. That includes AMT, but it also includes PTT."

He explained, "PTT is Intel's 'Run a TPM in software on the ME' feature. If you're using PTT and someone compromises your ME, the TPM is no longer trustworthy. That probably means your Bitlocker keys are compromised, but it also means all your remote attestation credentials are toast."

Garrett said if an exploit allows unsigned data to be installed and interpreted by the ME, an attacker could effectively trigger the reinfection of malware after every ME reboot. Were that to happen, the only way to fix things would be to reflash the hardware by hand. At that point, he said, it would probably be cheaper just to get new hardware.



The Register @TheRegister

Thanks, Intel.

9:39 PM - Nov 20, 2017

15 285 263

Intel said systems using ME Firmware versions 11.0, 11.5, 11.6, 11.7, 11.10, and 11.20, SPS Firmware version 4.0, and TXE version 3.0 are affected. The cited CVE-assigned bugs are as follows:

- **Intel Manageability Engine Firmware 11.0.x.x/11.5.x.x/11.6.x.x/11.7.x.x/11.10.x.x/11.20.x.x**
  - **CVE-2017-5705:** "Multiple buffer overflows in kernel in Intel Manageability Engine Firmware 11.0/11.5/11.6/11.7/11.10/11.20 allow attacker with local access to the system to execute arbitrary code." Logged-in superusers, or high-privilege programs, can execute code within the hidden Management Engine, below the OS and any other software.
  - **CVE-2017-5708:** "Multiple privilege escalations in kernel in Intel Manageability Engine Firmware 11.0/11.5/11.6/11.7/11.10/11.20 allow unauthorized process to access privileged content via unspecified vector." Logged-in users or running apps can slurp confidential information out of memory. This is very bad news on a shared system.
  - **CVE-2017-5711:** "Multiple buffer overflows in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allow attacker with local access to the system to execute arbitrary code with AMT execution privilege." Logged-in superusers, or high-privilege programs, can execute code within the AMT suite, below the OS and any other software.
  - **CVE-2017-5712:** "Buffer overflow in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allows attacker with remote Admin access to the system to execute arbitrary code with AMT execution privilege." People with network access to a machine, and can log in as an admin, can execute code within the AMT suite.
- **Intel Manageability Engine Firmware 8.x/9.x/10.x**
  - **CVE-2017-5711:** "Multiple buffer overflows in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allow attacker with local access to the system to execute arbitrary code with AMT execution privilege." Logged-in superusers, or high-privilege programs, can execute code within the AMT suite, below the OS and any other software.
  - **CVE-2017-5712:** "Buffer overflow in Active Management Technology (AMT) in Intel Manageability Engine Firmware 8.x/9.x/10.x/11.0/11.5/11.6/11.7/11.10/11.20 allows attacker with remote Admin access to the system to execute arbitrary code with AMT execution privilege." People with network access to a machine, and can log in as an admin, can execute code within the AMT suite.
- **Server Platform Service 4.0.x.x**
  - **CVE-2017-5706:** "Multiple buffer overflows in kernel in Intel Server Platform Services Firmware 4.0 allow attacker with local access to the system to execute arbitrary code." Logged-in superusers, or high-privilege programs, can execute code within the hidden Management Engine, below the OS and any other software.
  - **CVE-2017-5709:** "Multiple privilege escalations in kernel in Intel Server Platform Services Firmware 4.0 allows unauthorized process to access privileged content via unspecified vector." Logged-in users or running apps can slurp confidential information out of memory. This is very bad news on a shared system.
- **Intel Trusted Execution Engine 3.0.x.x**
  - **CVE-2017-5707:** "Multiple buffer overflows in kernel in Intel Trusted Execution Engine Firmware 3.0 allow attacker with local access to the system to execute arbitrary code." Logged-in superusers, or high-privilege programs, can execute code within the hidden Management Engine, below the OS and any other software.
  - **CVE-2017-5710:** "Multiple privilege escalations in kernel in Intel Trusted Execution Engine Firmware 3.0 allows unauthorized process to access privileged content via unspecified vector." Logged-in users or running apps can slurp confidential information out of memory. This is very bad news on a shared system.

Chipzilla thanked Mark Ermolov and Maxim Goryachy at Positive for discovering and bringing to its attention the flaw CVE-2017-5705, which sparked the aforementioned review of its source code for vulnerabilities.

Intel advises Microsoft and Linux users to download and run the Intel-SA-00086 detection tool to determine whether their systems are vulnerable to the above bugs. If you are at risk, you must obtain and install firmware updates from your computer's manufacturer, if and when they become available. The new code was developed by Intel, but it needs to be cryptographically signed by individual hardware vendors in order for it to be accepted and installed by the engine.

Lenovo was quick off the mark with patches for its gear ready to download.

We'll give you a roundup of fixes as soon as we can. It's not thought Apple x86 machines are affected as they do not ship with Intel's ME, as far as we can tell.

Today's news will no doubt fuel demands for Intel to ship components free of its Management Engine – or provide a way to fully disable it – so people can use their PCs without worrying about security bugs on mysterious secluded coprocessors. ®

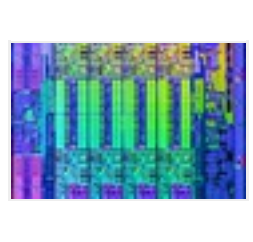
Sponsored: Advanced Threat Prevention. Visit The Register's Endpoint Security Hub

Tips and corrections | 79 Comments

Sign up to our Newsletter - Get IT in your inbox daily

MORE Intel Security Hardware

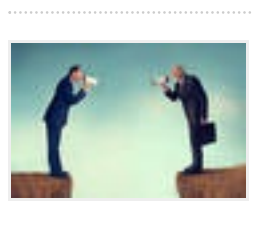
Most read


Intel finds critical holes in secret Management Engine hidden in tons of desktop, server chipsets


London mayor: Self-driving cars? Not without jacked-up taxes, you don't!


Wait, did Oracle tip off world to Google's creepy always-on location tracking in Android?

Microsoft's memory randomization security defense is a little busted in Windows 8, 10


Open-source defenders turn on each other in 'bizarre' trademark fight sparked by GPL fall out

More from The Register


Whomp. Intel's promised fatter Optane drive arrives
Offers advice on getting better Optane benchmark boosts


Intel is upset that Qualcomm is treating it like Intel treated AMD for years and years
Chipzilla takes number, joins queue to kick Snapdragon biz in the ball arrays

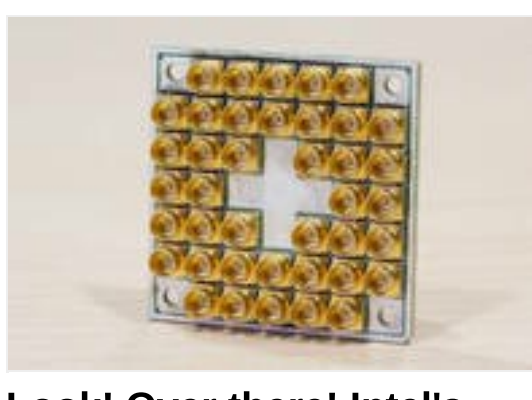

Ex-Intel boss Paul Otellini dead at age 66
Krzanich pays tribute to former Chipzilla supremo


Intel axes 140 IoTers in California, Ireland
Think of it as your independence day


Intel AMT bug bit Siemens industrial PCs
Patches issued for 38 products, plus bonus Web portal bug-fix


Intel's 8th-gen CPUs are called Ice Lake. And so are the 9th-gen
Chipzilla in overlapping naming weirdness mess


Billion-euro Intel EU antitrust saga goes on and on and...
European Court of Justice decides general court skipped important analysis


Look! Over there! Intel's cooked a 17-qubit chip quantum package
Have you tried collapsing the waveform and polarizing a photon again?

Whitepapers

Accelerating the business value of flash storage
Once you've decided to move to all-flash, you will quickly learn that not all flash systems are alike.

Legacy Decommissioning: Good for the Budget, Good for Compliance
Learn how migrating enterprise data stored in legacy applications onto a modern archive system can improve access, lower costs, and simplify compliance.

Preparing for the General Data Protection Regulation
For most organizations, the implications of GDPR are both significant and far-reaching.

Top Ten Criteria for Selecting a Managed Services Provider
How are you going to balance digital innovation with the risk of new technology infrastructure?

Sponsored links

Know Your Infrastructure - On Prem and in the Cloud

Advanced Threat Prevention. Visit The Register's Endpoint Security Hub

Get The Register's Headlines in your inbox daily - quick signup!

New from Avere - Cloud-Enabled Data Center for Dummies. Download now

The Register uses cookies. Find out more. Close