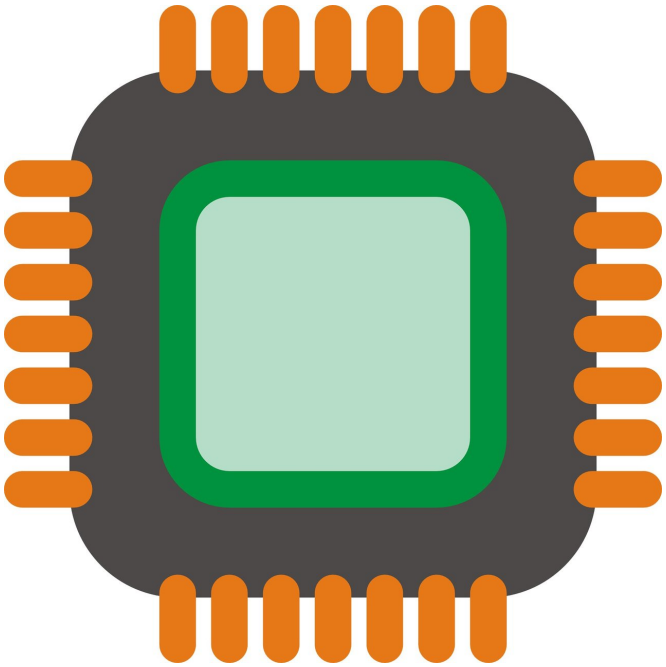
Intel Management Engine vulnerability is recognized

23 November 2017, by Nancy Owano



Credit: CC0 Public Domain

(Tech Xplore)—Intel has issued a security advisory with the severity rating of "Important."

The US-CERT (Computer Emergency Readiness Team) on the website of the US Department of Home Security has encouraged users and administrators to review several Intel links and refer to their original equipment manufacturers (OEMs) for mitigation strategies and updated firmware.

"Intel has released recommendations to address vulnerabilities in the firmware of the following Intel products: Management Engine, Server Platform Services, and Trusted Execution Engine. An attacker could exploit some of these vulnerabilities to take control of an affected system."

The Department of Homeland Security gave the guidance a day after Intel said it had identified security vulnerabilities in remote-management software known as "Management Engine," said Reuters.

The Reuters story was one of numerous reports about the Intel advisory and a focal point in concern was the Intel remote administration feature known as the Management Engine.

"The platform has a lot of useful features for IT managers," said Lily Newman in *Wired*, "but it requires deep system access that offers a tempting target for attackers," as a compromise could mean control of a computer.

The Management Engine is "to allow administrators to control devices remotely for all types of functions, from applying updates to troubleshooting," she wrote.

Businesses, said Reuters, were alerted as the Management Engine shipped with eight types of processors used in business computers.

The affected chips were said to be widely used. Jay Little, a security engineer with Trail of Bits, said in Reuters that the vulnerabilities affected business computers and servers with Intel processors sold in the last two years.

These computers are sold by names as Dell, Lenovo, Hewlett Packard Enterprise and other manufacturers, said Reuters.

Researchers outside of Intel had identified the problem.

"Intel would like to thank Mark Ermolov and Maxim Goryachy from Positive Technologies Research for working collaboratively with Intel on a coordinated disclosure and providing the initial finding for CVE-2017-5705, CVE-2017-5706 and CVE-2017-5707," said Intel.

Wired said Ermolov and Goryachy will present their findings at Black Hat Europe next month.

At Black Hat Europe 2017 in London, Ermolov, system programmer, is described on the event site as interested in security aspects of hardware, firmware, and low-level system software (bare-metal hypervisors, OSes cores, device drivers). The site said "he is researching various hardware components of Intel platforms: PCH, IOSF, iGPU, and corresponding firmware."

The Intel advisory was released on Nov. 20 and revised on Nov. 21.

In response to the researchers' findings, Intel said it "performed an in-depth comprehensive security review" of Intel Management Engine (ME), Server Platform Services (SPS), and Intel Trusted Execution Engine (TXE). The result of Intel's look: They identified security vulnerabilities "that could potentially place impacted platforms at risk." What could go wrong as a result?

Intel in its advisory said, "an attacker could gain unauthorized access to platform, Intel ME feature, and 3rd party secrets protected by the Intel Management Engine (ME), Intel Server Platform Service (SPS), or Intel Trusted Execution Engine (TXE)."

What now?

Reuters spelled it out. Intel spokesperson Agnes Kwan said the company had provided software patches to fix the issue to all major computer manufacturers. It was up to them to distribute patches to users.

Nonetheless, said Reuters, "Security experts noted that it could take time to fix vulnerable systems because installing patches on computer chips is a difficult process."

Ars Technica checked in for readers with an update as of November 22: HP, Dell, and other vendors completed patches for their firmware and are preparing them for distribution.

Intel published a detection tool so Windows and Linux administrators can check their systems.

Intel also said, "Contact your system manufacturer to obtain updates for impacted systems."

"These updates are available now," Intel said in a statement to *Wired*. "Businesses, systems administrators, and system owners using computers or devices that incorporate these Intel products should check with their equipment manufacturers or vendors for updates for their systems, and apply any applicable updates as soon as possible."

More information: Intel Q3'17 ME 11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update: security-center.intel.com/advi … 086&languageid=en-fr
Intel-SA-00086 Detection Tool: downloadcenter.intel.com/download/27150

APA citation: Intel Management Engine vulnerability is recognized (2017, November 23) retrieved 17 January 2022 from https://techxplore.com/news/2017-11-intel-vulnerability.html