Security

Intel's management engine - in most CPUs since 2008 - can be p0wned over USB

Creator of OS on the chip calls out Chipzilla for keeping his work secret

By Richard Chirgwin 9 Nov 2017 at 05:11 28 SHARE ▼

Positive Technologies, which in September said it has a way to attack the Intel Management Engine, has dropped more details on how its exploit works.

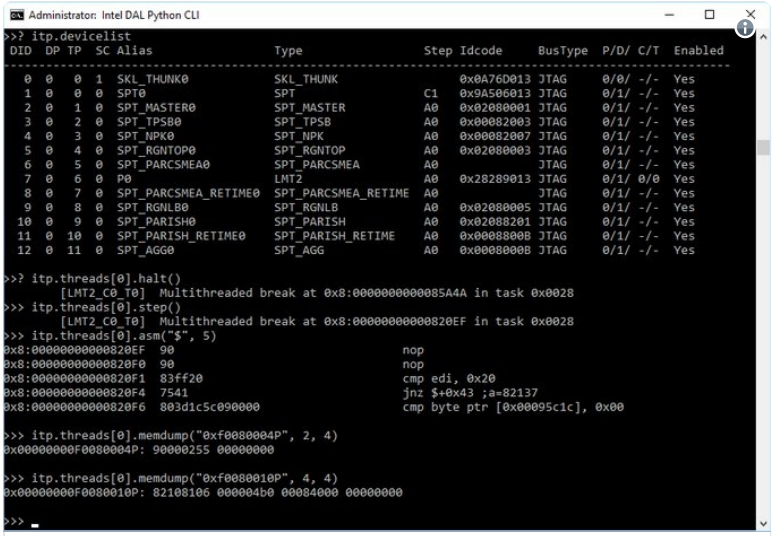
The firm has already promised to demonstrate God-mode hack in December 2017, saying the bug “allows an attacker of the machine to run unsigned code in the Platform Controller Hub on any motherboard”.

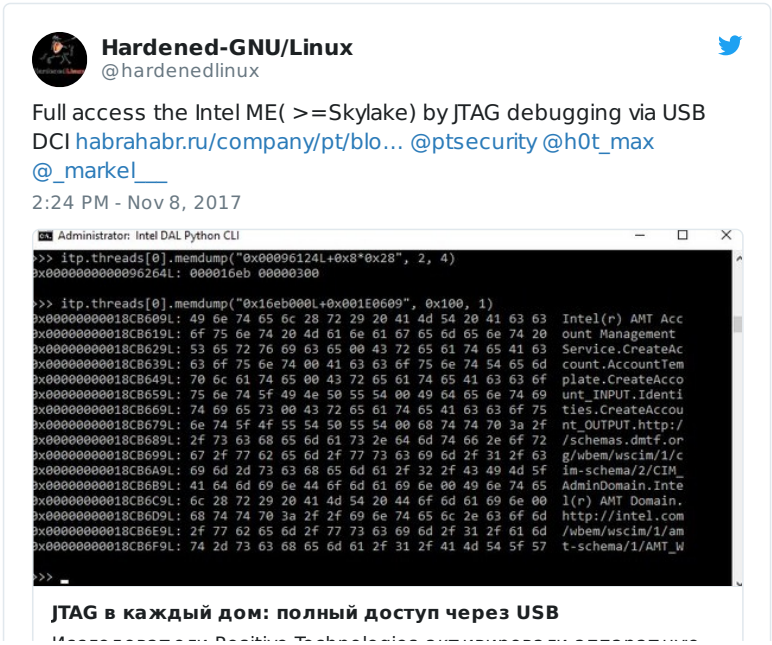
For some details, we'll have to wait, but what's known is bad enough: Intel Management Engine (IME) talks to standard Joint Test Action Group (JTAG) debugging ports. As does does USB, so Positive Technologies researchers put the two together and crafted a way to access IME from the USB port.

IME's problems first emerged in May, when researchers noticed you could access the Active Management Technology running on the microcontroller with an empty login string.

That was patchable, but the IME – a microcontroller that's got full control over hardware and networking, independently of the operating system – remained in place.

The latest attack came to Vulture South's attention via a couple of Tweets:





The linked blog post [in Russian] explains that since Skylake, the PCH – Intel's Platform Controller Hub, which manages chip-level communications – has offered USB access to JTAG interfaces that used to need specialised equipment. The new capability is DCI, Direct Connect Interface.

Any attack needs access to USB which as we know is really difficult.

We still don't know all the details Positive Technologies will show off at Black Hat, but their trailers are sure fun to watch. ®

Bootnote: The IME is able to control a computer because it runs an OS of its own, namely MINIX. And it turns out that while Intel talked to MINIX's creator about using it, the company never got around to saying it had put it into every CPU it makes.

Which has MINIX's creator, Andrew S. Tanenbaum, just a bit miffed. As Tanenbaum wrote this week in an open letter to Intel CEO Brian Krzanich:

> **The only thing that would have been nice is that after the project had been finished and the chip deployed, that someone from Intel would have told me, just as a courtesy, that MINIX was now probably the most widely used operating system in the world on x86 computers. That certainly wasn't required in any way, but I think it would have been polite to give me a heads up, that's all.**

Tips and corrections

28 Comments

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

MORE Usb

More from The Register

New Azure servers to pack Intel FPGAs as Microsoft ARM-lessly embraces Xeon

'Intel Xeon Scalable Processor' hailed as 'cornerstone for new platform' with servers customised for different roles

Microsoft, Intel cook kit to secure firmware in servers and beyond

Because everything has firmware and it survives reboots. PLUS: Redmond details HPE-killing cloud servers

Bing fling sting: Apple dumps Microsoft search engine for Google

Safari, Spotlight to be powered by the Chocolate Factory

Microsoft Edge shock: Browser opts for Apple WebKit, Google Blink

On iOS and Android, cough

Google cloud switches on Intel's Skylake Xeons and cloud CPU picker

Another thing cloud's changed: it used to be be server-makers that trumpeted CPU exclusives

Microsoft: We beat Google, AWS to cloudy GPU VMs in Blighty

Now you can shave a few milliseconds from real-time apps and, er, batch processing

Whitepapers

Sponsored links