



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:

Administrator: Intel DAL Python CLI

```
>>> itp.devicelist
-----
DID  DP  TP  SC  Alias                Type                Step Idcode    BusType  P/D/  C/T  Enabled
-----
0  0  0  1  SKL_THUNK0           SKL_THUNK           0x0A76D013    JTAG     0/0/  -/-  Yes
1  0  0  0  SPT0                 SPT                  C1            0x9A506013    JTAG     0/1/  -/-  Yes
2  0  1  0  SPT_MASTER0          SPT_MASTER          A0            0x02080001    JTAG     0/1/  -/-  Yes
3  0  2  0  SPT_IPSB0            SPT_IPSB            A0            0x00082003    JTAG     0/1/  -/-  Yes
4  0  3  0  SPT_NPK0             SPT_NPK             A0            0x00082007    JTAG     0/1/  -/-  Yes
5  0  4  0  SPT_RGNTOP0          SPT_RGNTOP          A0            0x02080003    JTAG     0/1/  -/-  Yes
6  0  5  0  SPT_PARCSMEA0        SPT_PARCSMEA        A0            JTAG       0/1/  -/-  Yes
7  0  6  0  P0                   LMT2                A0            0x28289013    JTAG     0/1/  0/0  Yes
8  0  7  0  SPT_PARCSMEA_RETIME0 SPT_PARCSMEA_RETIME A0            JTAG       0/1/  -/-  Yes
9  0  8  0  SPT_RGNLB0           SPT_RGNLB           A0            0x02080005    JTAG     0/1/  -/-  Yes
10 0  9  0  SPT_PARISH0          SPT_PARISH          A0            0x0208201     JTAG     0/1/  -/-  Yes
11 0 10 0  SPT_PARISH_RETIME0   SPT_PARISH_RETIME   A0            0x0008800B    JTAG     0/1/  -/-  Yes
12 0 11 0  SPT_AGG0             SPT_AGG             A0            0x0008000B    JTAG     0/1/  -/-  Yes

>>> itp.threads[0].halt()
[LMT2_C0_T0] Multithreaded break at 0x8:000000000085A4A in task 0x0028
>>> itp.threads[0].step()
[LMT2_C0_T0] Multithreaded break at 0x8:0000000000820EF in task 0x0028
>>> itp.threads[0].asm("$", 5)
0x8:0000000000820EF  90          nop
0x8:0000000000820F0  90          nop
0x8:0000000000820F1  83ff20     cmp edi, 0x20
0x8:0000000000820F4  7541       jnz $+0x43 ;a=82137
0x8:0000000000820F6  803d1c5c090000 cmp byte ptr [0x00095c1c], 0x00

>>> itp.threads[0].memdump("0xf080004P", 2, 4)
0x00000000f080004P: 90000255 00000000

>>> itp.threads[0].memdump("0xf080010P", 4, 4)
0x00000000f080010P: 82108106 000004b0 00084000 00000000

>>> _
```

Maxim Goryachy
@h0t_max



Hardened-GNU/Linux

@hardenedlinux



Full access the Intel ME(>=Skylake) by JTAG debugging via USB DCI [habrahabr.ru/company/pt/blo...](https://habrahabr.ru/company/pt/blog/251111/) @ptsecurity @h0t_max @_markel_

2:24 PM - Nov 8, 2017

```
Administrator: Intel DAL Python CLI
>>> itp.threads[0].memdump("0x0000000000000000", 2, 4)
0x0000000000000000: 000016eb 00000300

>>> itp.threads[0].memdump("0x16eb0000+0x001E0609", 0x100, 1)
0x0000000000000000: 49 6e 74 65 6c 28 72 29 20 41 4d 54 20 41 63 63 Intel(r) AMT Acc
0x0000000000000001: 6f 75 6e 74 20 4d 61 6e 61 67 65 6d 65 6e 74 20 ount Management
0x0000000000000002: 53 65 72 76 69 63 65 00 43 72 65 61 74 65 41 63 Service.CreateAc
0x0000000000000003: 63 6f 75 6e 74 00 41 63 63 6f 75 6e 74 54 65 6d count.AccountTem
0x0000000000000004: 70 6c 61 74 65 00 43 72 65 61 74 65 41 63 63 6f plate.CreateAcco
0x0000000000000005: 75 6e 74 5f 49 4e 50 55 54 00 49 64 65 6e 74 69 unt_INPUT.Identi
0x0000000000000006: 74 69 65 73 00 43 72 65 61 74 65 41 63 63 6f 75 tiles.CreateAccou
0x0000000000000007: 6e 74 5f 4f 55 54 50 55 54 00 68 74 74 70 3a 2f nt_OUTPUT.http:/
0x0000000000000008: 2f 73 63 68 65 6d 61 73 2e 64 6d 74 66 2e 6f 72 /schemas.dmtf.or
0x0000000000000009: 67 2f 77 62 65 6d 2f 77 73 63 69 6d 2f 31 2f 63 g/wbem/wscim/1/c
0x000000000000000a: 69 6d 2d 73 63 68 65 6d 61 2f 32 2f 43 40 4d 5f im-schema/2/CIM_
0x000000000000000b: 41 64 6d 69 6e 44 6f 6d 61 69 6e 00 49 6e 74 65 AdminDomain.Inte
0x000000000000000c: 6c 28 72 29 20 41 4d 54 20 44 6f 6d 61 69 6e 00 l(r) AMT Domain.
0x000000000000000d: 68 74 74 70 3a 2f 2f 69 6e 74 65 6c 2e 63 6f 6d http://intel.com
0x000000000000000e: 2f 77 62 65 6d 2f 77 73 63 69 6d 2f 31 2f 61 6d /wbem/wscim/1/am
0x000000000000000f: 74 2d 73 63 68 65 6d 61 2f 31 2f 41 4d 54 5f 57 t-schema/1/AMT_W
>>> _
```

JTAG в каждый дом: полный доступ через USB

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.

Sponsored: [The Joy and Pain of Buying IT - Have Your Say](#)

Tips and corrections

28 Comments

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

MORE [Usb](#)



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



The 3-Stage Journey To The All-Flash Cloud

Evolving to the all-flash cloud - and how your organisation can benefit at every stage in the journey.



Six Trends in Retail Analytics for 2017

2017's newest trends in retail and consumer goods analytics.



Scaling Customer Communications

Do CCM offerings need to change in response to the new generation of consumers?



Preparing for the General Data Protection Regulation

For most organizations, the implications of GDPR are both significant and far-reaching.

Sponsored links

[Get The Register's Headlines in your inbox daily - quick signup!](#)

About us>

- [Who we are](#)
- [Under the hood](#)
- [Contact us](#)
- [Advertise with us](#)

More content>

- [Week's headlines](#)
- [Top 20 stories](#)
- [Alerts](#)
- [Whitepapers](#)

Situation Publishing>

- [The Next Platform](#)
- [Continuous Lifecycle London](#)
- [M-cubed](#)
- [Webinars](#)



The Register - Independent news and views for the tech community. Part of Situation Publishing

Sign up to our Newsletters

Join our daily or weekly newsletters, subscribe to a specific section or set [News alerts](#)

Subscribe



Biting the hand that feeds IT © 1998–2017

[Cookies](#) [Privacy](#) [Ts&Cs](#)