More than 20GB of Intel source code and proprietary data dumped online

reader comments

59 with 50 posters participating, including story author

Share this story

Intel is investigating the purported leak of more than 20 gigabytes of its proprietary data and source code that a security researcher said came from a data breach earlier this year.

The data—which at the time this post went live was publicly available on BitTorrent feeds—contains data Intel makes available to partners and customers under NDA, a company spokeswoman said. Speaking on background, she said Intel officials don't believe the data came from a network breach. She also said the company is still trying to determine how current the material is and that, so far, there is no signs the data includes any customer or personal information.

"We are investigating this situation," company officials said in a statement. "The information appears to come from the Intel Resource and Design Center, which hosts information for use by our customers, partners and other external parties who have registered for access. We believe an individual with access downloaded and shared this data."

Exconfidential Lake

The data was published by Tillie Kottmann, a Swiss software engineer who offered barebones details on Twitter. Kottmann has dubbed the leak “exconfidential Lake,” with Lake being a reference to the Intel insider name for its 10 nanometer chip platform. They said they obtained the data from a source who breached Intel earlier this year and that today’s installment would be followed by others in the future.

“Most of the things here have NOT been published ANYWHERE before and are classified as confidential, under NDA or Intel Restricted Secret,” Kottmann wrote. They said some of the contents included:

- *Intel ME Bringup guides + (flash) tooling + samples for various platforms*
- *Kabylake (Purley Platform) BIOS Reference Code and Sample Code + Initialization code (some of it as exported git repos with full history)*
- *Intel CEFDK (Consumer Electronics Firmware Development Kit (Bootloader stuff)) SOURCES*
- *Silicon / FSP source code packages for various platforms*
- *Various Intel Development and Debugging Tools*
- *Simics Simulation for Rocket Lake S and potentially other platforms*
- *Various roadmaps and other documents*
- *Binaries for Camera drivers Intel made for SpaceX*
- *Schematics, Docs, Tools + Firmware for the unreleased Tiger Lake platform*
- *(very horrible) Kabylake FDK training videos*
- *Intel Trace Hub + decoder files for various Intel ME versions*
- *Elkhart Lake Silicon Reference and Platform Sample Code*
- *Some Verilog stuff for various Xeon Platforms, unsure what it is exactly.*

- *Debug BIOS/TXE builds for various Platforms*
- *Bootguard SDK (encrypted zip)*
- *Intel Snowridge / Snowfish Process Simulator ADK*
- *Various schematics*
- *Intel Marketing Material Templates (InDesign)*
- *Lots of other things*

Material as recent as May

A quick review of the leaked material shows that it consists of confidential materials that Intel customers need to design motherboards, BIOS, or other things that work with CPUs and other chips Intel makes. Although we're still analyzing the contents, we're seeing design and test documents, source code, and presentations ranging from as early to Q4 2018 to just a couple of months ago.

Most of these documents and source code packages apply to Intel CPU platforms, like Kaby Lake or the upcoming Tiger Lake, although there is a smattering of other documents relating to other products, such as a sensor package Intel developed for SpaceX.

There is also a folder dedicated to the Intel Management Engine, but its contents, too, aren't anything Intel integrators don't already know. They're test code and recommendations for when and how often to run those automated tests while designing systems that include an Intel CPU with the Intel ME.

One of the dump's newer bits included "Whitley/Cedar Island Platform Message of the Week," dated May 5. Cedar Island is the motherboard architecture that lies beneath both Cooper Lake and Ice Lake Xeon CPUs. Some of those chips were released earlier this year, while some have yet to become generally available. Whitley is the dual-socket architecture for both Cooper Lake (14nm) and Ice Lake (10nm) Xeons. Cedar Island is

for Cooper Lake only

The contents include plenty of diagrams and graphics like the one below:

Some contents provide a cryptic reference to voltage failures in some Ice Lake samples. It’s not clear if the failures apply to actual hardware delivered to customers or if they’re happening on reference boards Intel provided to OEMs for use in designing their own boards.

How done it?

While Intel said it doesn’t believe the documents were obtained through a network breach, a screenshot of the conversation Kottmann had with the source provided an alternate explanation. The source said that the documents were hosted on an unsecured server hosted on Akamai’s content delivery network. The source claimed to have identified the server using the nmap port-scanning tool and from there, used a python script to guess default passwords.

Here’s the conversation:

> *source: They have a server hosted online by Akami CDN that wasn't properly secure. After an internet wide nmap scan I found my target port open and went through a list of 370 possible servers based on details that nmap provided with an NSE script.*
>
> *source: I used a python script I made to probe different aspects of the server including username defaults and unsecure file/folder access.*
>
> *source: The folders were just lying open if you could guess the name of one. Then when you were in the folder you could go back to root and just click into the other folders that you didn't know the name of.*
>
> *deletescape: holy shit that's incredibly funny*
>
> *source: Best of all, due to another misconfiguration, I could masqurade as any of their employees or make my own user.*
>
> *deletescape: LOL*
>
> *source: Another funny thing is that on the zip files you may find password protected. Most of them use the password Intel123 or a lowercase intel123*
>
> *source: Security at it's finest.*

Kottmann said they didn't know the source well but based on the apparent authenticity of the material, there's no reason to doubt the source's account of how it was obtained.

The Intel spokeswoman didn't immediately provide a response to the claim.

Many onlookers have expressed alarm that the source code has comments containing the word "backdoor." Kottmann told Ars that the word appeared two times in the source code associated with Intel's Purely Refresh chipset for Xeon CPUs. So far,

there are no known analyses of the source code that have found any covert methods for bypassing authentication, encryption, or other security protections. Besides, the term backdoor in coding can sometimes refer to debugging functions or have other benign meanings.

People are also lampooning the use of the passwords Intel123 and intel123. These are no doubt weak passwords, but it’s unlikely their purpose was to secure the contents of the archive files from unauthorized people.

https://arstechnica.com/?p=1697330