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

By Dan Goodin

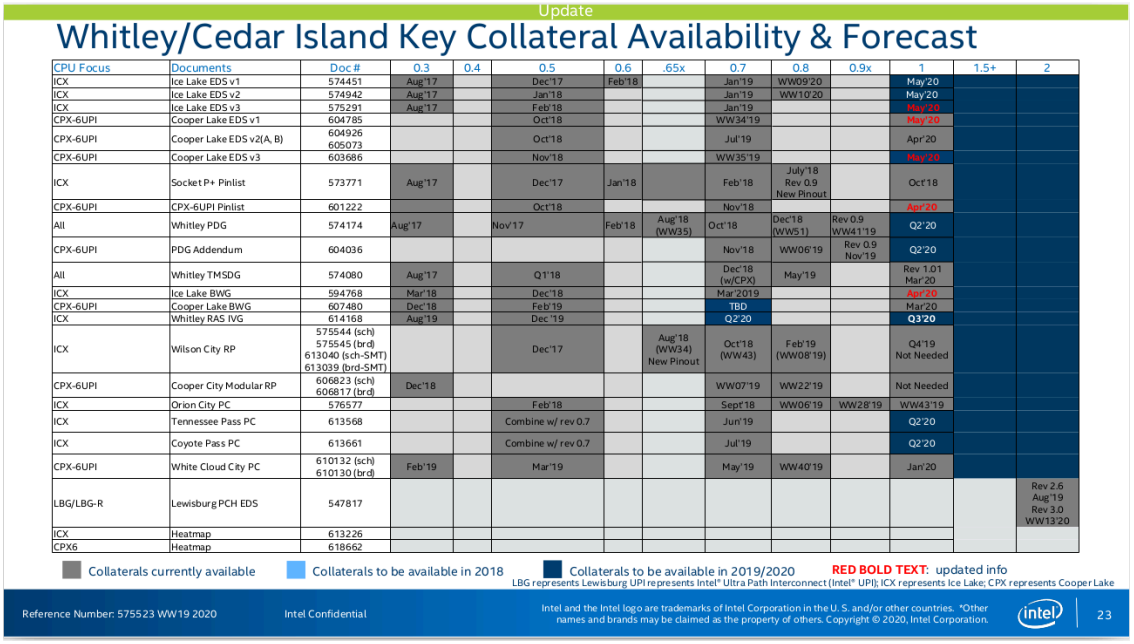
Published: 2020-08-06 · Archived: 2026-04-05 21:05:04 UTC

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:



CPU Focus	Documents	Doc #	0.3	0.4	0.5	0.6	.65x	0.7	0.8	0.9x	1	1.5+	2
ICX	Ice Lake EDS v1	574451	Aug'17		Dec'17	Feb'18		Jan'19	WW09'20		May'20		
ICX	Ice Lake EDS v2	574942	Aug'17		Jan'18			Jan'19	WW10'20		May'20		
ICX	Ice Lake EDS v3	575291	Aug'17		Feb'18			Jan'19			May'20		
CPX-6UPI	Cooper Lake EDS v1	604785			Oct'18			WW34'19			May'20		
CPX-6UPI	Cooper Lake EDS v2(A, B)	604926 605073			Oct'18			Jul'19			Apr'20		
CPX-6UPI	Cooper Lake EDS v3	603686			Nov'18			WW35'19			May'20		
ICX	Socket P+ Pinlist	573771	Aug'17		Dec'17	Jan'18		Feb'18	July'18 Rev 0.9 New Pinout		Oct'18		
CPX-6UPI	CPX-6UPI Pinlist	601222			Oct'18			Nov'18			Apr'20		
All	Whitley PDG	574174	Aug'17		Nov'17	Feb'18	Aug'18 (WW35)	Oct'18	Dec'18 (WW51)	Rev 0.9 WW41'19	Q2'20		
CPX-6UPI	PDG Addendum	604036						Nov'18	WW06'19	Rev 0.9 Nov'19	Q2'20		
All	Whitley TMSDG	574080	Aug'17		Q1'18			Dec'18 (w/CPX)	May'19		Rev 1.01 Mar'20		
ICX	Ice Lake BWG	594768	Mar'18		Dec'18			Mar'2019			Apr'20		
CPX-6UPI	Cooper Lake BWG	607480	Dec'18		Feb'19			TBD			Mar'20		
ICX	Whitley RAS IVG	614168	Aug'19		Dec'19			Q2'20			Q3'20		
ICX	Wilson City RP	575544 (sch) 575545 (brd) 613040 (sch-SMT) 613039 (brd-SMT)			Dec'17		Aug'18 (WW34) New Pinout	Oct'18 (WW43)	Feb'19 (WW08'19)		Q4'19 Not Needed		
CPX-6UPI	Cooper City Modular RP	606823 (sch) 606817 (brd)	Dec'18					WW07'19	WW22'19		Not Needed		
ICX	Orion City PC	576577			Feb'18			Sept'18	WW06'19	WW28'19	WW43'19		
ICX	Tennessee Pass PC	613568			Combine w/ rev 0.7			Jun'19			Q2'20		
ICX	Coyote Pass PC	613661			Combine w/ rev 0.7			Jul'19			Q2'20		
CPX-6UPI	White Cloud City PC	610132 (sch) 610130 (brd)	Feb'19		Mar'19			May'19	WW40'19		Jan'20		
LBG/LBG-R	Lewisburg PCH EDS	547817											Rev 2.6 Aug'19 Rev 3.0 WW13'20
ICX	Heatmap	613226											
CPX6	Heatmap	618662											

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.

Source: https://arstechnica.com/information-technology/2020/08/intel-is-investigating-the-leak-of-20gb-of-its-source-code-and-private-data/