KB4100347: Intel microcode updates

Summary

Recent Changes:

- Intel Microcode updates around the following products (CPUs) have been revised. We recommend that you take this latest update to stay current:
  - Nehalem EP, Nehalem WS
  - Lynnfield
  - Lynnfield Xeon
  - Arrandale
  - Clarkdale
  - Clarkdale Xeon
  - WestmereEP, WS

Intel recently announced that it has completed its validations and started to release microcode for recent CPU platforms related to Spectre Variant 2 (CVE 2017-5715 ["Branch Target Injection"]). This update includes microcode updates from Intel for the following CPUs:

Product name (CPU)	Public name	CPUID	Intel Microcode update revision
Skylake H/S	6th Generation Intel Core Processor Family	506E3	0xC2
Skylake U/Y & Skylake U23e	6th Generation Intel Core m Processors	406E3	0xC2
Skylake Server SP (H0, M0, U0)	Intel® Xeon® Bronze Processor 3104, 3106	00050654	0x2000049

	Intel® Xeon® Gold Processor 5115, 5118, 5119T, 5120, 5120T, 5122, 6126, 6126F, 6126T, 6128, 6130, 6130F, 6130T, 6132, 6134, 6134M, 6136, 6138, 6138F, 6138T, 6140, 6140M, 6142, 6142F, 6142M, 6144, 6146, 6148, 6148F, 6150, 6152, 6154, Intel® Xeon® Platinum Processor 8153, 8156, 8158, 8160, 8160F, 8160M, 8160T, 8164, 8168, 8170, 8170M, 8176, 8176F, 8176M, 8180, 8180M, Intel® Xeon® Silver Processor 4108, 4109T, 4110, 4112, 4114, 4114T, 4116, 4116T		
Skylake D (Bakerville)	Intel® Xeon® Processor D-2123IT, D-2141I, D-2142IT, D2143IT, D-2145NT, D-2146NT, D-2161I, D-2163IT, D2166NT, D-2173IT, D-2177NT, D-2183IT, D-2187NT	00050654	0x2000049

Skylake X (Basin Falls)	Intel® Core™ i9 79xxX, 78xxX	00050654	0x2000049
Kaby Lake U	7th Generation Intel® Core™ Mobile Processors	000806E9	0x84
Kaby Lake U23e	7th Generation Intel® Core™ Mobile Processors	000806E9	0x84
Kaby Lake Y	7th Generation Intel® Core™ Mobile Processors	000806E9	0x84
KBL-R U	8th Generation Intel® Core™ Mobile Processor Family	000806EA	0x84
Kaby Lake G	7th Generation Intel® Core™ Processor Family	000906E9	0x84
Kaby Lake H	7th Generation Intel® Core™ Processor Family	000906E9	0x84
Kaby Lake S	7th Generation Intel® Core™ Processor Family	000906E9	0x84
Kaby Lake X	7th Generation Intel® Core™ Processor Family	000906E9	0x84
Kaby Lake Xeon E3	7th Generation Intel® Core™ Processor Family	000906E9	0x84

Coffee Lake H 6+2	8th Generation Intel® Core™ Processor Family	000906EA	0x84
Coffee Lake S 6+2	8th Generation Intel® Core™ Processor Family	000906EA	0x84
Coffee Lake S 6+2 Xeon E3	8th Generation Intel® Core™ Processor Family	000906EA	0x84
Coffee Lake S 6+2 x/KBP	8th Generation Intel® Core™ Processor Family	000906EA	0x84
Coffee Lake S (4+2)	8th Generation Intel® Core™ Desktop Processor Family	000906EB	0x84
Broadwell DE A1	Intel® Xeon® Processor D-1513N, D-1523N, D-1533N, D-1543N, D1553N	50665	0xE000009
Broadwell DE V1	Intel® Xeon® Processor D-1520, D-1540	50662	0x15
Broadwell DE V2,V3	Intel® Xeon® Processor D-1518, D-1519, D-1521, D-1527, D-1528, D-1531, D-1533, D-1537, D-1541, D-1548, Intel® Pentium® Processor D1507, D1508, D1509, D1517, D1519	50663	0x7000012

Broadwell DE Y0	Intel® Xeon® Processor D-1557, D-1559, D-1250, D-1571, D-1577, D-1581, D-1587	50664	0xF000011
Broadwell H 43e	Intel® Core™ Processor i7-5950HQ, i7-5850HQ, i7-5750HQ, i7-5700HQ, Intel® Core™ Processor i5-5575R, i5-2505C, i5-2505R, i7-5775C, i7-5775R, Intel® Core™ Processor i7-5700EQ, i7-5850EQ	40671	0x1D
Broadwell U/Y	Intel® Core™ Processor i7-5650U,i7-5600U, i7-5557U, i7-5550U, i7-5500U, Intel® Core™ Processor i5-5350U, i5-5350,i5-5300U, i5-5287U,i5-5257U, i5-5250U, i5-5200U, Intel® Core™ Processor i3-5157U, i3-5020U, i3-5015U, i3-5010U, i3-5006U, i3-5005U, i3-5010U, i5-5350U, i7-5650U, Intel® Core™ Processor M-5Y71, M-5Y70, M-5Y51, M-5Y3, M-	306D4	0x2A

	5Y10c, M -5Y10a, M-5Y10, Intel® Pentium® Processor 3805U, 3825U, 3765U, 3755U, 3215U, 3205U, Intel® Celeron® 3765U		
Broadwell Xeon E3	Intel® Xeon® Processor v4 E3-1258L, E3-1265L, E3-1278L, E3-1285, E3-1285	40671	0x1D
Broadwell Server E, EP, EP4S	Intel® Xeon® Processor E5-2603V4, E5-2609V4, E5- 2620V4, E5-2623V4, E5-2630LV4, E5-2630V4, E5- 2637V4, E5-2640V4, E5-2643V4, E5-2650LV4, E5- 2650V4, E5-2660V4, E5-2667V4, E5-2679V4, E5-2680V4, E5-2683V4, E5-2690V4, E5-2695V4, E5-2697AV4, E5-2697V4, E5-2698V4, E5-2699AV4, E5-2699V4	406F1	0xB00002C

	Intel® Xeon® Processor E5-2608LV4, E5-2618LV4, E5- 2628LV4, E5-2648LV4, E5-2658V4, E5-2699RV4, E5- 4628LV4		
Broadwell Server EX	Intel® Xeon® Processor E7-4809V4, E7-4820V4, E7- 4830V4, E7-4850V4, E7-8855V4, E7-8860V4, E7-8867V4, E7-8870V4, E7-8880V4, E7-8890V4, E7-8891V4, E7-8893V4, E7-8894V4	406F1	0xB00002C
Haswell (including H, S), Xeon E3	4th Generation Intel® Core™ Mobile Processor Family, Intel® Pentium® Mobile Processor Family, Intel® Celeron® Mobile Processor Family	306C3	0x24
Haswell Perf Halo	Intel® Core™ Extreme Processor (5960x, 5930x, 5820x)	40661	0x19
Haswell Server E, EP, EP4S	Intel® Xeon® Processor v3 E5-1428L, E5-1603	306F2	0x3C

	E5-1607, E5-1620, E5-1630, E5-1650, E5-1660, E5-1680, E5-2408L, E5-2418L, E5-2428L, E5-2438L, E5-2603, E5-2608L, E5-2608L, E5-2609, E5-2618L, E5-2620, E5-2623, E5-2628L, E5-2630, E5-2630L, E5-2637, E5-2640, E5-2643, E5-2648L, E5-2650, E5-2650L, E5-2658, E5-2660, E5-2667, E5-2670, E5-2680, E5-2683, E5-2685, E5-2687W,E5-2690, E5-2695, E5-2697, E5-2698, E5-2699, E5-4610, E5-4620, E5-4627, E5-4640, E5-4648, E5-4650, E5-4655, E5-4660, E5-4667, E5-4669		
Haswell ULT	4th Generation Intel® Core™ Mobile Processor Family, Intel® Pentium® Mobile Processor Family, Intel® Celeron® Mobile Processor Family	40651	0x23
Ivy Bridge	3rd Generation Intel® Core™ Mobile Processor Family, Intel® Pentium® Mobile Processor	306A9	0x1F

	Family, and Intel® Celeron® Mobile Processor Family		
Ivy Bridge Xeon E3	Intel® Core™ Processor Extreme Edition i7-4960X Intel® Core™ Processor i7-4820K, i7-4930K	306A9	0x1F
Ivy Bridge E, Ivy Bridge Server E, EN, EP, EP4S	Intel® Xeon® Processor v2 E5-1428L, E5-1620, E5-1650, E5-1660, E5-2403, E5-2407, E5-2418L, E5-2420, E52428L, E5-2430, E5-2430L, E5-2440, E5-2448L, E5-2450, E5-2450L, E5-2470, E5-2603, E5-2609, E5-2618L, E52620, E5-2628L, E5-2630, E5-2630L, E5-2637, E5-2640, E5-2643, E5-2648L, E5-2650, E5-2650L, E5-2658, E52660, E5-2667, E5-2670, E5-2680, E5-2687W, E5-2690, E5-2695, E5-2697, E5-4603, E5-4607, E5-4610, E5-4620, E5-4624L, E5-4627, E5-4640, E5-4650, E5-4657L	000306E4	0x42C
Ivy Bridge Server EX	E5-4610, E5-4620, E5-4624L, E5	000306E7	0x713

	4627, E5-4640, E54650, E5-4657L		
Sandy Bridge	Intel® Core™ i3-21xx/23xx-T/M/E/UE Processor, Intel® Core™ i5-23xx/24xx/25xx-T/S/M/K Processor, Intel® Core™ i7-2xxx-S/K/M/QM/LE/UE/QE Processor, Intel® Core™ i7-29xxXM Extreme Processor, Intel® Celeron® Desktop G4xx, G5xx Processor, Intel® Celeron® Mobile 8xx, B8xx Processor, Intel® Pentium® Desktop 350, G6xx, G6xxT, G8xx Processor, Intel® Pentium® Mobile 9xx, B9xx Processor	206A7	0x2D
Sandy Bridge Xeon E3	Intel® Xeon® Processor E3-1200 Product Family	206A7	0x2D
Sandy Bridge Server EN/EP/EP4S	Intel® Xeon® Processor E5-2620, E5-2630, E5-2630L, E52640, E5-2650, E5-2650L, E5-2660, E5-2667, E5-2670, E5-2680, E5-2690	206D6	0x61C

Sandy Bridge Server EN/EP/EP4S	Intel® Xeon® Processor E5-1428L, E5-1620, E5-1650, E51660, E5-2403, E5-2407, E5-2418L, E5-2420, E5-2428L, E5-2430, E5-2430L, E5-2440, E5-2448L, E5-2450, E52450L, E5-2470, E5-2603, E5-2609, E5-2620, E5-2630, E5-2630L, E5-2637, E5-2640, E5-2643, E5-2648L, E52650, E5-2650L, E5-2658, E5-2660, E5-2665, E5-2667, E5-2670, E5-2680, E5-2687W, E5-2690, E5-4603, E54607, E5-4610, E5-4617, E5-4620, E5-4640, E5-4650,E5-4650L Intel® Pentium® Processor 1405	206D7	0x713
Knights Landing	Intel® Xeon® Phi™ Processor 72xx	50671	0x1B6
Knights Mill	Intel® Xeon® Phi™ Processor Family	80650	0x18
Nehalem EP, Nehalem WS	Intel® Xeon® Processor E5502, E5503, E5504, E5506, E5507, E5520, E5530, E5540 Intel® Xeon® Processor L5506, L5508, L5518, L5520, L5530	106A5	0x1C

	Intel® Xeon® Processor W5580, W5590 Intel® Xeon® Processor X5550, X5560, X5570		
Lynnfield	Intel® Core™ Processor i7-860, 860S, 870, 870S, 875K, 880 Intel® Core™ Processor i5-750, 750S, 760	106E5	0x09
Lynnfield Xeon	Intel® Xeon® Processor L3426 Intel® Xeon® Processor X3430, X3440, X3450, X3460, X3470, X3480	106E5	0x09
Arrandale	Intel® Core™ Processor i7-i7-620M/LM/UM, i7-640LM/UM Intel® Core™ Processor i5-430M, i5-520M/UM, i5-540M Intel® Core™ Processor 330M, 350M Intel® Celeron® Processor P4500, P4505	20652	0x10

Clarkdale	Intel® Core™ Processor i5-650, 660, 661, 670 Intel® Core™ Processor i3-530, 540, 550, 560 Intel® Pentium® Processor G6950	20652	0x10
Clarkdale Xeon	Intel® Xeon® Processor L3406	20652	0x10
Arrandale	Intel® Core™ Processor i7-610E, 620LE/LM/M/UE/UM, 640LM/M/UM, 660LM/UE/UM, 680UM Intel® Core™ Processor i5-430M/UM, 450M, 460M, 470UM, 480M, 520E/M/UM, 540M/UM, 560M/UM, 580M Intel® Core™ Processor i3-330E/M/UM, 350M, 370M, 380M/UM, 390M Intel® Pentium® Processor P6000, P6100, P6200, P6300 Intel® Pentium® Processor U5400, U5600	20655	0x6

	Intel® Celeron® Processor P4500, P4505, P4600 Intel® Celeron® Processor U3400, U3405, U3600		
Clarkdale	Intel® Core™ Processor i5-650, 655K, 660, 661, 670, 680 Intel® Core™ Processor i3-530, 540 Intel® Pentium® Processor G6950, G6951, G6960	20655	0x6
WestmereEP, WS	Intel® Xeon® Processor E5603, E5606, E5607, E5620, E5630, E5640, E5645, E5649 Intel® Xeon® Processor L5609, L5618, L5630, L5638, L5640 Intel® Xeon® Processor W3670, W3680 Intel® Xeon® Processor X5647, X5650, X5660, X5667, X5670, X5672, X5675, X5677, X5680, X5687, X5690, X5698	206C2	0x1E

This update is a standalone update targeted for Windows 10 version 1803 (Windows 10 April 2018 Update) and Windows Server Version 1803 (Server Core). This update also includes Intel microcode updates that were already released for these operating systems at the time of release to manufacturing (RTM). We will offer additional microcode updates from Intel through this article for these operating systems as they become available to Microsoft. This mitigation is on by default for Windows client systems so no action is required. Please ensure that mitigation against Spectre Variant 2 is enabled for servers through the registry settings that are documented in the following article:

Windows Server guidance to protect against speculative execution side-channel vulnerabilities

> **Important**
>
> Consult with your device manufacturer and Intel via their websites regarding their microcode recommendation for your device before applying this update to your device.

How to obtain and install the update

Method 1: Windows Update

To download and install this update, go to **Settings** > **Update & Security** > **Windows Update** and then select **Check for updates**. If Windows Update says your device is up to date, you have all the updates that are currently available.

Method 2: Windows Server Update Service

This update is now available for installation through WSUS.

Method 3: Microsoft Update Catalog

To get the stand-alone package for this update, go to the Microsoft Update Catalog website.

More Information

How to obtain help and support for this security update

Last Updated: Jan 8, 2019