Cisco C880 M5 with Xeon Platinum 8100 CPU Release Notes (1.0.4)

Firmware Revision: 1.0.4
First Published: April 18, 2018
Last Updated: July 17, 2018

Introduction

Cisco C880 M5 with Xeon Platinum 8100 CPU is an 8-Socket x86 Rack servers. It will be based on eight Intel® Xeon® Platinum 8100 series processors with max memory of 3TB or 6TB or 9TB or 12TB. SAP HANA Certifications will be done by Cisco on this product and this will be managed by UCS Director.

System Requirements

There are no specific system requirements for this release of firmware.

New and Changed Features

There is no specific change in any of the software features.

Changes in Behavior

There are no specific change in any of the software feature and their behavior.

Scalability Improvements

There is no specific improvement in any of scalability requirements.

Related Documentation

The documents specifically for Cisco C880 M5 server with Xeon Platinum 8100 CPU are located at specified link:

http://www.cisco.com/c/en/us/products/servers-unified-computing/c880-m5-server/index.html

Installation and Upgrade Notes

The installation module and upgrade notes are located in the released firmware bundle. The following table maps firmware release versions with individual components.

Release Version	BIOS Version	iRMC Version	note
1.0.1	1.27.0	01.21C	Initial release
1.0.2	1.27.0	01.29C	
1.0.3	1.57.0	01.42C	Address CVE-2017-5715 (Spectre/Variant 2)
1.0.4	1.64.0	01.48C	Address the following CVEs: CVE-2018-3639 – Speculative Store Bypass (SSB) – also known as Variant 4 CVE-2018-3640 – Rogue System Register Read (RSRE) – also known as Variant 3a

Upgrade Paths

The firmware release package can be downloaded from specified link:

http://www.cisco.com/cisco/web/support/index.html

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account. For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Bugs for This Release

All open bugs for this release are available in the Cisco Bug Search Tool through the open bug search (https://bst.cloudapps.cisco.com/bugsearch/).

That search includes workarounds for the following open bugs, if any, and any additional open bugs.

Bug ID	Headline

Bug ID	Headline
---------	**[Description]** [BIOS Online Update] The online update of BIOS firmware fails on the iRMC WebUI. Restriction: The online update of BIOS firmware is not available. To be resolved in future iRMC firmware. **[Workaround]** Please use BIOS Offline Update. [Internal ID: i1]
--------	**[Description]** [kernel panic] Kernel Panic may occur by using the programs which issue many AVX512 instructions, when the Turbo mode is enabled. Under investigation **[Workaround]** Please disable Turbo mode in the system by BIOS menu. [Internal ID: S3, R3]
--------	**[Description]** [Messages at booting] The following message may be output to OS console and "/var/log/messages" during booting SLES12SP2. ---------- systemd-udevd[xxxx]: Assertion '!d->current' failed at src/libsystemd/sd-event/sd-event.c:702, function event_unmask_signal_data(). Aborting. kernel: Core dump to |/usr/lib/systemd/systemd-coredump xxx...xxx systemd-udevd pipe failed No plan to solve. **[Workaround]** No functional issue. Ignore the message. The update for kernel has been provided to suppress the error message. Recommended update for systemd : SUSE-RU-2017:0709-1 https://www.suse.com/support/update/announcement/2017/suse-ru-20170709-1/ [Internal ID: S5]
--------	**[Description]** RHEL7.3 with 4TB or more memory Unable to boot RHEL7.3 on the system with 4TB or more memory. Solved with errata (RHSA-2017-0386). The errata has been provided. https://access.redhat.com/solutions/2858351 **[Workaround]** Add "dhash_entries=0x20000000 ihash_entries=0x10000000" in kernel option. [Internal ID: R6]

Bug ID	Headline
--------	**[Description]** [Install] To install RHEL7.3 may fail due to NMI watchdog at 1st reboot. No plan to solve. **[Workaround]** Set “pmtmr=0” in grub.conf. 1. Push "e" key to edit grub.conf in Grub monitor. 2. Add kernel parameter "pmtmr=0" to grub.conf. 3. Boot the system. [Internal ID: R7]
--------	**[Description]** [Sub NUMA Clustering] The following message may be output to OS console and "/var/log/messages" during booting RHEL7.3, when the SNC (Sub NUMA Clustering) function is enabled. ---------- "WARNING: CPU: x PID: x at ../arch/x86/kernel/smpboot.c:xxx topology_sane.isra" Under investigation **[Workaround]** No functional issue. Please ignore the message. [Internal ID: R8]
CSCvk28595	**[Description]** If you set “Address range mirror” memory mode, this problem would happen. Memory operation mode setting changes unexpectedly from “Address range mirror” to “Full mirror” after following event. - System AC OFF and AC ON, or (*) - iRMC reboot (*) AC OFF and ON is disconnecting and reconnecting all AC cords from the system. **[Workaround]** None.

Resolved Bugs for This Release

Bug ID	Headline
CSCvh66783	A security issue related to CVE listed below is mitigated at this Release 1.0.3. Cisco C880 M5 servers are based on Intel® Xeon® Scalable Processors (Skylake) that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as Spectre and Meltdown. • CVE-2017-5753 (Spectre/Variant 1) is addressed by applying relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5715 (Spectre/Variant 2) is addressed by applying the updated microcode included in the C880 M5 servers as well as the relevant Operating System and Hypervisor patches from the appropriate vendors. • CVE-2017-5754 (Meltdown) is addressed by applying the relevant Operating System patches from the appropriate vendors. This release includes BIOS revisions for Cisco C880 M5 generation server. These BIOS revisions include the updated microcode that is a required part of the mitigation for CVE-2017-5715 (Spectre/Variant 2).
CSCvj59127	A security issue related to CVE listed below is mitigated at this Release 1.0.4 (BIOS 1.64.0). SpectreNG · CVE-2018-3639 – Speculative Store Bypass (SSB) – also known as Variant 4 · CVE-2018-3640 – Rogue System Register Read (RSRE) – also known as Variant 3a This release includes BIOS revisions for Cisco C880 M5 generation server. These BIOS revisions include the updated microcode that is a required part of the mitigation for CVE-2018-3639 and 3640 (Variant 4 and 3a).
CSCvk52609	“Onboard LAN disabled“ setting causes hardware error during BIOS POST. This is fixed at this Release 1.0.4 (BIOS 1.64.0). BIOS POST does not work properly under the condition of “Onboard_LAN_Controller = disabled“. Therefore, an Operating System does not wake up. This results in a SEL record below. Tue Apr 10 03:49:10 2018 | Critical | 0A0000 | **Undetermined system hardware failure**
CSCvk56475	Some standard MIB objects included incorrect strings. This is fixed at this Release 1.0.4 (iRMC 1.48C). SNMP OID (1.3.6.1.2.1.1) which iRMC firmware returns contains incorrect character strings. These strings are fixed as below. (underlined parts) .iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0 = STRING: C880M5 Tue May 22 11:11:29 JST 2018 .iso.org.dod.internet.mgmt.mib-2.system.sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.28.1

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.