Cisco C880 M4 with E7-8800 v3 CPU Release Notes (1.2.7)

Firmware Revision: BB18061
First Published: December 15, 2015
Last Updated: July 17, 2018

Introduction

Cisco C880 M4 with E7-8800 v3 CPU is an 8-Socket x86 Rack servers. It will be based on eight Intel® Xeon® E7-8880 v3 series processors with max memory of 2TB or 6TB. SAP HANA Certifications will be done by Cisco on this products 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 behaviour.

Scalability Improvements

There is no specific change in any of scalability requirements.

Related Documentation

The documents specifically for Cisco C880 M4 server with E7-8800 v3 CPU are located at specified link:

http://www.cisco.com/c/en/us/products/servers-unified-computing/c880-m4-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	Firmware Version	BIOS Version	BMC Version	MMB Version
1.2.1	BB15114	1.48	2.08	20.45
1.2.2	BB16021	1.52	2.09	20.48
1.2.3	BB16036	1.58	2.13	20.91
1.2.4	BB16053	1.59	2.14	20.57 (*)
1.2.5	BB17034	1.69	2.22	30.41
1.2.6	BB18031	1.77	2.23	30.46
1.2.7	BB18061	1.82	2.23	30.47

(*) Even though revision number is smaller than previous one, revision 20.57 is newer.

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 (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

CSCur60300	**[Description]** When you go to MMB Web-UI: >System >DU > DU#x, or >Disk Enclosure > Disk Enclosure#x, The latest status of RAID card, Physical Drives, and Logical Drives shown in the table does not appear immediately. **[Workaround]** Status of RAID card, Physical Drives, and Logical Drives is polled every 1 minute, so it will take maximum 1 minute to show the latest status. Note: If “Disk Enclosure#x” does not appear, please click “System” in the navigation bar to refresh display after the system enters boot state.
CSCuy48445	**Description** [MMB Web-UI] The page of "Disk Enclosure" is not displayed in MMB Web-UI in case that no logical drive is configured on the RAID controller.. **Workaround** No plan to solve.
CSCuy48536	**[Description]** [Video Redirection] Unable to open the video redirection after firmware update. **[Workaround]** No plan to solve. Execute the following CLI command. *set bmccontrol reset VR <sb#>*

Resolved Bugs for This Release

Bug ID	Headline
CSCuy41727	**Description** [Network Configuration] C880-M4 - Alarm E-Mail gives HTTP 500 error if FQDN is used for SMTP srv **Workaround** Use IP address instead of FQDN.

CSCve49104	**[Phenomenon]** Video redirection function of C880 M4 (with E7-8800 v2/v3/v4 CPU) can not be started with a client PC which Java version shown below is installed on. - Java 8 update131 or later **[Cause]** Modifications below are applied in Java 8 update131. Authentication method of MD5-signed JAR file is changed at Java 8 update 131. Because video redirection function of C880 M4 uses MD5 signature, this Java modification causes the problem. **[Workaround]** (1) Please do not update to this version if you use Video redirection of C880 M4. OR (2) If you have already installed Java 8 update 1.31 or later, please follow the below. Please modify the Java related file on a PC. It is not necessary to reboot PC after editing the file. - Windows PC (*) C:\Program Files\Java\jre1.8.0_131\lib\security\java.security - Linux client (*) /usr/java/jre1.8.0_131/lib/security/java.security (*) This example above is in case of default installation path - edit a line: 573 as shown Before editing: jdk.jar.disabledAlgorithms=MD2, MD5, RSA keySize < 1024 After editing: jdk.jar.disabledAlgorithms=MD2, RSA keySize < 1024
----------	Security issues related to CVE-IDs listed below are fixed at this Release 1.2.5 (Firmware BB17034). Vulnerabilities related to OpenSSL CVE-2016-0797, CVE-2016-2105, CVE-2016-2106, CVE-2016-2108, CVE-2016-2109, CVE-2015-1789, CVE-2015-1790, CVE-2015-1792, CVE-2015-1791, CVE-2014-8176, CVE-2016-2183 Vulnerabilities related to ntpd CVE-2015-8138, CVE-2016-1550, CVE-2016-2516, CVE-2016-2517, CVE-2016-2519, CVE-2016-2518, CVE-2015-8139, CVE-2015-7973, CVE-2015-8140, CVE-2016-1549, CVE-2015-7978, CVE-2015-8158, CVE-2015-7977, CVE-2015-7979, CVE-2016-1547
----------	Security issues related to CVE-IDs listed below are fixed at this Release 1.2.6 (Firmware BB18031). Vulnerabilities related to MMB firmware OS kernel CVE-2011-1076, CVE-2012-3552, CVE-2011-1927, CVE-2011-1581, CVE-2011-4087 Vulnerabilities related to MMB firmware - glibc: CVE-2016-10228 - logrotate: CVE-2011-1154, CVE-2011-1155, CVE-2011-1098 - net-snmp: CVE-2015-5621, CVE-2014-2284, CVE-2012-6151
----------	This fix is related to MMB Configuration backup/restore function on MMB Web-UI. MMB Configuration backup/restore function did not backup/restore setting items of “Remote Server Management“. Firmware BB18031 resolves this.

CSCvh66783	A security issue related to CVE listed below is mitigated at this Release 1.2.6 (Firmware BB18031). Cisco C880 M4 servers are based on Intel® Xeon® E7-8800 v3 series processors 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 M4 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 M4 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 1.2.7 (BIOS 1.82). 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 M4 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).

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.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)