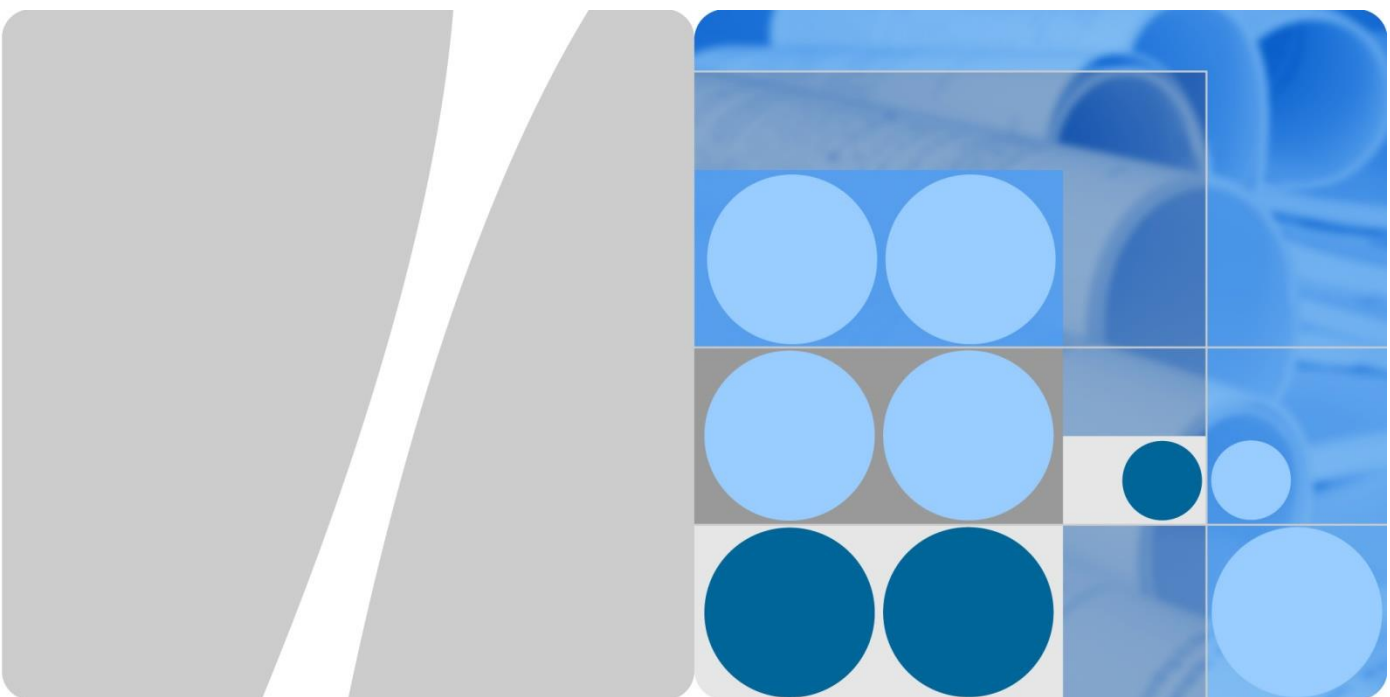




CH242 V3

iBMC V399 Release Notes

Issue	01
Date	2021-08-21

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://enterprise.huawei.com>

Contents

1 V399 Release Notes 1

2 V398 Release Notes 2

3 V323 Release Notes 5

4 V320 Release Notes 7

5 V311 Release Notes 9

6 V308 Release Notes 10

7 V298 Release Notes 12

8 V268 Release Notes 14

9 V235 Release Notes 17

10 V233 Release Notes 18

11 V231 Release Notes 19

12 V230 Release Notes 20

13 V218 Release Notes 22

14 V208 Release Notes 24

15 V202 Release Notes 25

16 V186 Release Notes 27

17 V180 Release Notes 28

18 V167 Release Notes 29

1 V399 Release Notes

Release Date

2021-08-21

Current Version

V399

Software Version

3.99

Earlier Version

V398

What's New

- Supports the DNS rebinding prevention function;
- Optimized the hard disk alarm mechanism;
- Optimized the CPLD protection mechanism of the BMC;
- Enhanced the reliability of user information.

Precautions

- If the iBMC version is 3.20 or earlier, upgrade it to version 3.23;
- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

2 V398 Release Notes

Release Date

2021-02-07

Current Version

V398

Software Version

3.98

Earlier Version

V323

What's New

- Optimized the IPMI command response mechanism;
- Supports setting and query of the SSH weak encryption algorithms through the Redfish interface;
- Optimized the memory and CPU information displayed on the WebUI;
- Optimized the VMM data transmission mechanism;
- Optimized the drive health status information on the WebUI;
- Enhanced web security;
- Optimized the suggestion for handling the fan fault alarm (alarm code: 0x04000007);
- Optimized the mechanism for reporting RAID controller card information;
- Supports dynamic configuration of the speed adjustment policy through the Redfish interface;
- Supports syslog messages in RFC3164 format;
- Supports collection of DFL logs by using the CLI;
- Optimized the trap reporting mechanism;
- Optimized the NVMe drive identification mechanism;
- Supports query of EnclosureID and Slot Number over the Redfish interface;
- Supports detection of the intermittent disconnection events of service NICs;
- Optimized the mechanism for obtaining the drive SNs;

- Optimized the mechanism for the mainboard CPLD upgrade to take effect;
- Added the function of triggering a warm restart of the OS when an IERR is detected in FDM;
- Optimized the power capping mechanism;
- Optimized the mechanism for updating the database of the intelligent fault management system;
- Optimized the alarm mechanism for connecting or disconnecting the optical cables of optical modules;
- Optimized the time zone displayed for New Zealand on the iBMC WebUI;
- Optimized the display of physical drives of the RAID array on the iBMC WebUI;
- Optimized the HTTPS access mechanism for security purposes;
- Changed the certificate expiry event to a minor alarm;
- Optimized the import and export of the LDAP configuration;
- Optimized the SSDP packet broadcast mechanism;
- Supports change of the rights for the user whose ID is 2;
- Optimized the alarm mechanism for the BBU in-position status of the RAID controller card;
- Added the function of triggering a warm reset of the operating system when the IERR diagnosis fails;
- Optimized the mechanism for logging the memory CE storm events;
- Optimized the FDM PFAE alarm mechanism;
- Supports SR450C-M 2G RAID controller cards;
- Supports successful VNC connections even in network delay;
- After hostname is configured using SmartKit, the SNMP sysname can be automatically synchronized with the new hostname;
- Removed the inconsistency between the drive SEL and the information displayed on the front panel LCD;
- Optimized the drive check and alarm mechanism;
- Optimized the mechanism for the SNMP to create the algorithm based on the engine ID;
- Optimized the mechanism for importing and exporting the BIOS configuration on the WebUI;
- Optimized the mechanism for handling the CPLD firmware upgrade exceptions on the WebUI;
- Optimized the event subscription enabling mechanism for the Redfish module;
- Optimized the mechanism for the Redfish interface to report the StatusChange event when a PSU is removed or installed;
- Optimized the SP boot process from the BMC;
- Optimized the commands used to configure the gateway IP address;
- Optimized the mechanism of managing multiple RAID cards;
- Optimized the mechanism of querying FRU information using ipmitool;
- Optimized the CPU card cooling policy;
- Optimized SNMP communication mechanism with third-party network management software;
- Provides the port connection view on the WebUI;
- Optimized the SNMP engine ID generation mechanism to solve the problem that the SNMP V3 probability is not connected;
- Optimized the cooling strategy of the GPU card;
- Optimized SSL-enabled cipher suites;
- Optimized the scheme of mounting ISO image by the CLI;
- Added support for the gratuitous ARP function;
- Optimized the processing mechanism of the SYN flood attack to solve the problem that the attack causes the probability reset of the BMC;

- Optimized the fixability scheme when the network port fails;
- Optimized the verification policy for SMTP mailbox names;
- Optimized the fault code display scheme;
- Added support for querying and setting UUIDs by the redfish interface;
- Optimized the monitoring strategy for memory usage;
- Added support the data security erasure for encrypted disks;
- Optimized the Chinese and English switching strategies when WEB logs in;
- Optimized WEB help information for occupancy monitoring;
- Optimized the configuration export mechanism;
- Optimized the authentication policy of SNMPV3.

Precautions

- If the iBMC version is 3.20 or earlier, upgrade it to version 3.23;
- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

3

V323 Release Notes

Release Date

2019-05-06

Current Version

V323

Software Version

3.23

Earlier Version

V320

What's New

- Optimized the cooling strategy of the GPU card;
- Optimized the mechanism for logging the memory CE storm events;
- Optimized the mechanism for the iBMC to report the Version Change event when the iBMC restarts;
- Optimized the periodic event update mechanism over the Redfish interface;
- Optimized the mechanism for importing and exporting the BIOS configuration on the WebUI;
- Optimized the FDM message processing mechanism;
- Optimized the FDM PFAE alarm mechanism.

Precautions

- If the iBMC version is 3.20 or earlier, upgrade it to version 3.23;
- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;

- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

4 V320 Release Notes

Release Date

2018-11-01

Current Version

V320

Earlier Version

V311

What's New

- Added support for time synchronization of NTP service on Windows;
- Added support for IPMI command to turn off the password rules long SNMP community name;
- Added support for the redfish interface to query the maximum number of PCIE cards;
- Added support for the redfish interface to query the maximum number of CPUs;
- Added support for the redfish interface to query the maximum number of hard disks;
- Added support for the redfish interface to query the maximum number of power supplies;
- Added support for the redfish interface to query the maximum number of fans;
- Added support for configuring LDAPS authentication options;
- Added support for CPU, memory, and hard disk log information after component replacement;
- Added support for querying and setting UUIDs by the redfish interface;
- Added support the data security erasure for encrypted disks;
- Optimized user management policies;

- Optimized component upgrade strategies;
- Optimized the out-of-band management scheme for storage devices;
- Optimized friendly information prompts when user deletion fails;
- Optimized the out-of-band alarm policy of the hard disk in multiple RAID scenarios;
- Optimized French help information on KVM;
- Optimized the remaining life detection mechanism of the NVMe hard disk;
- Optimized the strategy of a virtual keyboard mouse to wake up a hibernated operating system;
- Optimized the implementation mechanism of the BMC restart button on the WEB page.
- Optimized the QPI/UPI alarm policy;
- Optimized the verification policy of the LDAP server address on the WEB page;
- Optimized the configuration import and export strategy;
- Optimized the FDM diagnostic process;
- Optimized the information display on the status bar and menu bar on the KVM;
- Optimized the out-of-band management for RAID Card;
- Optimized NCSI network configuration features;
- Optimized the verification policy for SMTP mailbox names;
- Optimized the fault code display scheme;
- Optimized the monitoring strategy for memory usage;
- Optimized the Chinese and English switching strategies when WEB logs in.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC;

5 V311 Release Notes

Release Date

2018-08-12

Current Version

V311

Earlier Version

V308

What's New

Rectified the security risks found.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

6 V308 Release Notes

Release Date

2018-07-12

Current Version

V308

Earlier Version

V298

What's New

- Optimized the secure login strategy;
- Optimized multi-language description of the "Disable Panel Power Button" switch on the WEB page;
- Optimized the scanning strategy of the management health sensor;
- Optimized SNMP encryption and SNMP V3 TRAP alarm reporting mechanism;
- Optimized the component information display scheme of the software RAID in the CLI and WEB;
- Optimized the description of the alarm event of the optical module and add the subject of the event to the description information;
- Optimized the service port configuration policy on the BMC;
- Optimized the information prompt when modifying the default password;
- Optimized the configuration information in the "version.xml" configuration file to be compatible with the umate and esight upgrade scenarios;
- Optimized the information display on the French interface help page;
- Optimized the configuration import policy and solve the problem that the configuration file cannot be imported again after importing invalid format files in some scenarios;

- Optimized rules for setting user login time on the WEB page;
- Optimized the working mode detection mechanism on the BMC;
- Optimized the display of the body type in the filter bar of the SEL page;
- Optimized the Firefox browser compatibility strategy to solve the problem of entering only the part of the user name in some scenarios;
- Optimized the language package upgrade strategy to solve the problem that the upgrade cannot be performed when there are special characters in the upgrade file name;
- Optimized memory alarm strategy;
- Added support for KVM-compatible Japanese keyboard functionality;
- Added support for obtaining the CPU clock frequency through the redfish interface;
- Added support for PCIE card BDF information acquisition;
- Added support for SSDP to report the ProductName function;
- Added support for using ipmiutil tools for enabled/disabled user functions;
- Added support for LDAP certificate chain authentication;
- Added support for the virtual media mounted via HTTPS Protocol;
- Added support for compatibility with the ipmiutil tool in the VMware system.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

7 V298 Release Notes

Release Date

2018-04-12

Current Version

V298

Earlier Version

V268

What's New

- Supports query of the BMC uptime and KVM token value through the Redfish interface;
- Supports query of RAID controller, disk, and temperature summary through the Redfish interface;
- Supports the operation of disabling the SNMPv2c write permission through the Redfish interface;
- Provides support for French on the WebUI;
- Allows security logs and operation logs to be cleared using the command line interface (CLI);
- Supports monitoring of the endurance of SSD media;
- Displays the slot number and chassis number of compute nodes on the WebUI;
- Supports monitoring and alarming of memory, QPI, and PCIe correctable error (CE) overflow;
- Supports upload of upgrade files using the Redfish POST operation;
- Enables multiple BIOS configurations performed through the Redfish interface to take effect at a time;
- Optimized the LDAP user login procedure;

- Optimized the NVMe disk information displayed on the WebUI;
- Optimized the OAM alarm check mechanism to prevent the iBMC from generating false alarms in certain scenarios;
- Modified the description of RAID card firmware version;
- Modified the description of the disk rate in the redfish interface;
- Modified the RTC voltage alarm threshold;
- Optimized the SNMPv1/v2 user login procedure;
- Optimized the pCIeDeviceDevicename information displayed under the pcieDevice node in SNMP;
- Optimized the WebUI display in Japanese;
- Optimized the PCIe card information displayed on the WebUI;
- Optimized the Time Zone page on the WebUI to prevent duplicate city names;
- Improved the reliability of file transfer between the management modules and compute nodes;
- Eliminated the one-click information collection failures by reducing the size of the video file;
- Optimized the procedure of the network driver in receiving abnormal packets;
- Modified the system reset event log description;
- Optimized the disk vendor information displayed on the WebUI;
- Supports automatic start of the OS after the OS is shut down due to CPU overtemperature;
- Enhanced FDM, including fault collecting, analysis, and diagnosis.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

8

V268 Release Notes

Release Date

2017-11-20

Current Version

V268

Earlier Version

V235

What's New

- Added support for the MZ520 and MZ522 NICs;
- Added to the iBMC IP address and SN to the KVM screen;
- Added support for daylight saving time;
- Added support for querying BOM codes;
- Added the status attribute of the Manager resources of Redfish;
- Added the NIC OAM detection function;
- Added support for using the SOL function through the CLI;
- Added support for querying and configuring the DST;
- Added the LDAP proxy user authentication function. The LDAP proxy account and password can be configured;
- Added the function of disabling accounts that are inactive for a specified period of time;
- Added the function of ejecting remote virtual devices in the OS;
- Allowed the LDAP configuration to support the Lithuania language;
- Optimized the LDAP login based on IPv6;

- Optimized the LDAP login of independent KVM clients so that special characters are allowed;
- Optimized the LDAP login time;
- Optimized the LDAP login method in IPv6 mode;
- Optimize the LDAP configuration to solve the problem that the LDAP user group configuration fails if the group is in the root directory;
- Optimized the time display of emails sent by the BMC so that the alarm event time is consistent with the BMC time;
- Optimized the KVM usage scenario to solve the virtual media connection failure during port mapping;
- Optimized the OID display in SNMP traps;
- Optimized the iBMC login method so that iBMC can be accessed after the host name is modified;
- Optimized the restart prompt displayed on the iBMC upgrade page;
- Optimized the prompt displayed during the resolution configuration on Ibmc;
- Optimized the CLI-based virtual media mounting so that the virtual media is automatically ejected after being used;
- Optimized the display of out-of-band RAID management;
- Optimized the import method of customized level-3 certificate chains on Ibmc;
- Optimized the SNMP v1/v2 community name login mode;
- Optimized the iBMC self-signed certificate time to be consistent with the local time;
- Optimized the factory settings restoration and added support for deleting operation logs;
- Optimized Redfish alarm levels so that they are consistent with alarms reported by other interfaces;
- Optimized the IPv6 address display to solve the problem that the IP address is empty during IPv6 address configuration;
- Optimized the user experience of non-full-screen remote KVM to solve the following problem: When the user uses arrow keys to operate the VMware menu bar on the left, the scroll bar on the right also moves;
- Optimized the messages displayed when the user imports an SSL certificate, imports a configuration file, or clicks the restart button on the upgrade page;
- Optimized the resolution prompt;
- Optimized the virtual CD/DVD ejection to solve the problem that the server repeated boots from CD/DVD after the CD/DVD ejection fails;
- Optimized the time required to log in to iBMC using LDAP;
- Optimized the web log filtering function to solve the problem that the filtered contents are occasionally incorrect;
- Optimized the CPU configuration detection mechanism so that the system displays a warning message when no CPU is installed;

- Optimized the RAID configuration function of Redfish to solve the problem that RAID cannot be created using default parameters;
- Optimized the memory ECC event logging scheme;
- Optimized the prompts on the firmware upgrade page on the WebUI;
- Optimized the virtual CD/DVD-ROM insertion and ejection on the KVM screen;
- Optimized the description of the watchdog timeout event log on the BMC;
- Optimized the format display of sensor names in the trap event code mode;
- Solved the abnormal web page display in the German language;
- Solved the severe vulnerability World writable files exist (unix-world-writable-files) found by Nexpose scan.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

9

V235 Release Notes

Release Date

2017-07-04

Current Version

V235

Earlier Version

V233

What's New

- iBMC logins by LDAP users are optimized: Full name logins are allowed. All users of subgroups of an LDAP group domain can log in;
- Integer chain import is supported.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

10 V233 Release Notes

Release Date

2017-03-28

Current Version

V233

Earlier Version

V231

What's New

- The WOL setting is optimized;
- SSL certificates can be imported through the CLI.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

11

V231 Release Notes

Release Date

2017-02-20

Current Version

V231

Earlier Version

V230

What's New

The Wake on Lan configuration is supported.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

12 V230 Release Notes

Release Date

2017-01-12

Current Version

V230

Earlier Version

V218

What's New

- Deleted the support for telnet to enhance security;
- Optimized the user account lock mechanism. User accounts will be locked when the number of incorrect password attempts reaches the limit;
- Supported import of the SSL certificates containing special character "-";
- Optimized LDAP implementation to enable iBMC access with LDAP login name and multi-level directory supported by user groups;
- Supported query of SSD disk endurance and firmware information;
- Supported query of DIMM type and SN information;
- Supported query of information about the number of CPU cores, total number of threads, cache size, and processor ID;
- Supported start of the remote console using the Java Network Launch Protocol (JNLP);
- Supported query of ES3000 V3 card information, such as the SN, model, endurance, and firmware version;
- The BMC supports use of the KVM function on the FREE BSD;
- Two-factor authentication via web is supported;
- The BMC supports OpenLDAP on Linux;
- The BMC supports enable and disable of the local KVM;
- The BMC supports RAID controller card alarm detection during the system start process.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

13

V218 Release Notes

Release Date

2016-10-18

Current Version

V218

Earlier Version

V208

What's New

- Upgraded the FDM function to version 2.1 to enhance the system error locating capability;
- Added the support for SSH public key authentication (PKA);
- Added the CLI login function for LDAP users;
- Optimized the IPMI module to support ipmitool 1.8.14;
- Enhanced security so that Telnet is disabled by default for newly created users;
- Enhanced security by prompting users to change the default password upon login;
- Enhanced security by allowing each BMC account to log in to only one web session at a time;
- Set the KVM cursor acceleration to be enabled by default to better synchronize the local and remote cursors;
- Optimized the KVM so that it supports more JRE versions, uses the CA signature certificate by default, and provides better user experience for PCs connected through the Internet;
- Optimize the KVM keyboard processing mechanism, solve the Tab key in the remote KVM inside the probability of failure;
- Solved the following problem: When RAID 1 is configured with an LSI SAS2308 controller card on the E9000, the BMC does not report alarms for removal of a member disk of RAID 1;

- Solved the following problem: The CPU and memory overtemperature alarms are always displayed on the intelligent chassis display of the E9000, but the actual temperatures are not high. The alarms are triggered by power shortage;
- Enabled LDAP to support the NTLM protocol;
- Eliminated the low probability that packet loss occurs when a PC pings the BMC management IP address;
- Solved the following problem: The keyboard does not work on the KVM screen if the local client runs SUSE 11;
- Solved the following problem: Magic keys do not work if ipmitool is used to log in over SOL to a server running Linux;
- Solved the following problem: Disk0 status queried through the IPMI interface is "unknown";
- resolve the problem that the CPU information queried by HMM is UNKNOWN;
- Added the function of supporting Ubuntu system clients on the remote virtual KVM;
- Added the function of supporting Ubuntu system clients on the remote virtual KVM;
- Resolved problem that when the client is a desktop cloud system, the "Num""caps" and "scroll" keys on the remote virtual KVM take effect only after being held down;
- Added the support for ES3000 V3 cards;
- Solved the silk screen parsing problem that occurs when PCIe faults are injected into PCIe SSDs.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

14 V208 Release Notes

Release Date

2016-07-16

Current Version

V208

Earlier Version

V202

What's New

- Optimized the WebUI and the description of the KVM power-on and power-off. The description is clearer;
- Optimized password security by prohibiting empty passwords;
- Optimized the SSL certificate import function. Resolved the problem that after the CSR file is generated for multiple times, importing the certificate fails;
- Users in customer role group can execute one-click collection on WebUI;
- Optimized the web online help to solve the low-probability problem that online help cannot be displayed properly;
- Optimized the enginetime mechanism of SNMP traps to solve the problem that some NMSs encounter errors in receiving SNMP traps;
- Added the support for E5-2618L v4 and E5-2658 v4 CPUs;
- Added the support for the MCIA card.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later;
- iBMC 2.08 or later does not support users with empty passwords. If iBMC is upgraded from an earlier version to 2.08 or later, users with empty passwords cannot log in to iBMC.

15 V202 Release Notes

Release Date

2016-04-12

Current Version

V202

Earlier Version

V186

What's New

- Added the function for starting the remote console through URL;
- Added the function for managing Broadwell E5 v4 series CPUs;
- Added the LDAP multi-domain management function (up to three LDAP servers can be configured);
- Added the support for the Japanese keyboard in KVM;
- Added the JRE version download link on a page of the iBMC web system;
- Added the function for disconnecting the KVM upon timeout;
- Added the function for using the ipmitool command to set an SNMP community name;
- Added the functions for querying and configuring the SNMP Trap mode;
- Added the SD card management function;
- Optimized the fault diagnosis function to enable users to correctly locate faulty components;
- Resolved the occasional reconnection failures upon abnormal SOL disconnections;
- Resolved the failure to enable the MZ220、MZ910、MZ912 during port power-on;
- Resolved the occasional garbled characters in SOL log files downloaded from the web system;
- Resolved the problem that the BMC is abnormal due to the long-time use of the SNMP client;
- Resolved system power-off failures upon the execution of the shutdown -h now command on operating systems;

- Resolved the problem that iBMC cannot power on or off devices after server power-on and power-off;
- Resolved the problem that incorrect RAID controller card quantities are occasionally displayed on the iBMC WebUI;
- Resolved the BMC function errors caused by log compression failures that occasionally occur;
- Optimized the compatibility with the FreeIPMI tool to resolve the problem that errors are reported when users query iBMC FRU information on the OS;
- Optimized the compatibility between MIB files and Spectrum to resolve Spectrum's failure to compile MIB files;
- Optimized the policy for adjusting the speed of mezzanine card fans;
- Optimized the MCE and CAT ERROR diagnosis function;
- Optimized the out-of-band management of PCIe SSDs so that users can query SSD information such as capacity and manufacturers;
- Installed the official SNMP software patch to defend against the 05840BRG vulnerability of SNMP 5.7.3.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later.

16 V186 Release Notes

Release Date

2015-12-27

Current Version

V186

Earlier Version

V180

What's New

- The BMC is abnormal due to the long-time use of the SNMP client;
- Resolved the failure to enable the MZ220、MZ910、MZ912 during power-on;
- Resolved the occasional reconnection failures upon abnormal SOL disconnections.

Precautions

- The BIOS software and complex programmable logical device (CPLD) software must be upgraded together;
- The MM910 software version needs to be upgraded to 5.12 or later.

17

V180 Release Notes

Release Date

2015-12-18

Current Version

V180

Earlier Version

V167

What's New

The following issue has been resolved: The BMC fails to connect to the VMware vCenter Server management platform.

Precautions

NA

18 V167 Release Notes

Release Date

2015-07-07

Current Version

V167

Earlier Version

NA

What's New

This issue is the first official release.

Precautions

NA

19 Vulnerability Patch List

Software Name	Software Version	CVE Number	CVSS Score	Vulnerability Description	Fixed Version
curl	7.69.1	CVE-2020-8286	7.5	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.	V399
curl	7.69.1	CVE-2020-8285	7.5	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.	V399
curl	7.69.1	CVE-2020-8284	3.7	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.	V399
curl	7.69.1	CVE-2021-22876	5.3	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an	V399

				Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.	
curl	7.69.1	CVE-2021-22897	5.3	curl 7.61.0 through 7.76.1 suffers from exposure of data element to wrong session due to a mistake in the code for CURLOPT_SSL_CIPHER_LIST when libcurl is built to use the Schannel TLS library. The selected cipher set was stored in a single "static" variable in the library, which has the surprising side-effect that if an application sets up multiple concurrent transfers, the last one that sets the ciphers will accidentally control the set used by all transfers. In a worst-case scenario, this we	V399
curl	7.69.1	CVE-2021-22898	7.5	curl 7.7 through 7.76.1 suffers from an information disclosure when the <code>-t` command line option, known as <code>`CURLOPT_TELNETOPTI ONS`</code> in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending <code>NEW_ENV</code> variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.</code>	V399
curl	7.69.1	CVE-2021-22890	3.7	curl 7.63.0 to and including 7.75.0 includes vulnerability that allows a malicious	V399

				HTTPS proxy to MITM a connection due to bad handling of TLS 1.3 session tickets. When using a HTTPS proxy and TLS 1.3, libcurl can confuse session tickets arriving from the HTTPS proxy but work as if they arrived from the remote server and then wrongly "short-cut" the host handshake. When confusing the tickets, a HTTPS proxy can trick libcurl to use the wrong session ticket resume for the host and thereby circumv	
PHP	7.3.22	CVE-2020-7069	6.5	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.	V399
PHP	7.3.22	CVE-2020-7070	5.3	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.	V399
PHP	7.3.22	CVE-2020-7071	7.5	In PHP versions 7.3.x below 7.3.26, 7.4.x below 7.4.14 and 8.0.0, when validating URL with functions like filter_var(\$url, FILTER_VALIDATE_URL), PHP will accept an URL with invalid password as valid URL. This may lead to functions that rely on URL	V399

				being valid to mis-parse the URL and produce wrong data as components of the URL.	
json-c	0.12.1	CVE-2020-12762	7.8	json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.	V399
openssh	8.2p1	CVE-2020-14145	5.9	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.	V399
openssh	8.2p1	CVE-2021-28041	7.1	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.	V399
openssh	8.2p1	CVE-2020-14145	5.9	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.	V399
openssh	8.2p1	CVE-2021-28041	7.1	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as	V399

				unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.	
TinyUI 2	2.34.0	CVE-2015-9251	6.1	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.	V398
TinyUI 2	2.34.0	CVE-2019-11358	6.1	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	V398
NTP	4.2.8p15	CVE-2019-11331	8.1	Network Time Protocol (NTP), as specified in RFC 5905, uses port 123 even for modes where a fixed port number is not required, which makes it easier for remote attackers to conduct off-path attacks.	V398
NTP	4.2.8p15	CVE-2018-8956	5.3	ntpd in ntp 4.2.8p10, 4.2.8p11, 4.2.8p12 and 4.2.8p13 allow remote attackers to prevent a broadcast client from synchronizing its clock with a broadcast NTP server via soofed mode 3 and mode 5 packets. The attacker must either be a part of the same broadcast network or control a slave in that broadcast network that can capture certain required packets on the attacker's behalf and send them to the attacker.	V398
NTP	4.2.8p15	CVE-2020-11868	7.5	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated	V398

				synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.	
OpenLDAP	2.4.49	CVE-2017-9287	6.5	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.	V398
OpenLDAP	2.4.49	CVE-2005-2069	5.0	pam_ldap and nss_ldap, when used with OpenLDAP and connecting to a slave using TLS, does not use TLS for the subsequent connection if the client is referred to a master, which may cause a password to be sent in cleartext and allows remote attackers to sniff the password.	V398
OpenLDAP	2.4.49	CVE-2017-14159	4.7	slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a "kill `cat /pathname`" command, as demonstrated by openldap-initscript.	V398
OpenLDAP	2.4.49	CVE-2017-17740	7.5	contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a	V398

				denial of service (slapd crash) via a member MODDN operation.	
OpenLDAP	2.4.49	CVE-2019-13565	7.5	An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption, and relying on the SASL security layers in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identity covered in those ACLs. After the first SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, this can affect different types of operations (searches, modify)	V398
OpenLDAP	2.4.49	CVE-2019-13057	4.9	An issue was discovered in the server in OpenLDAP before 2.4.48. When the server administrator delegates rootDN (database admin) privileges for certain databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from requesting authorization as an identity from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configuration to deploy a system where the server administrator and a DB administrator)	V398
OpenLDAP	2.4.49	CVE-2009-3767	4.3	libraries/libldap/tls_o.c in OpenLDAP 2.2 and 2.4, and possibly other versions, when OpenSSL is used, does not properly handle a '\0' character in a domain name in	V398

				the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	
OpenLDAP	2.4.49	CVE-2020-12243	7.5	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	V398
OpenLDAP	2.4.49	CVE-2015-3276	5.0	The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.	V398
OpenLDAP	2.4.49	CVE-2020-15719	4.2	libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.	V398
curl	7.69.1	CVE-2020-8169	7.5	curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure vulnerability that can lead to a partial password being leaked over the network and to the DNS server(s).	V398
curl	7.69.1	CVE-2020-	7.1	curl 7.20.0 through 7.70.0 is vulnerable to improper r	V398

		8177		restriction of names for files and other resources that can lead to overwriting a local file when the -J flag is used.	
curl	7.69.1	CVE-2020-8231	7.5	Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.	V398
PHP	7.3.22	CVE-2017-7272	7.4	PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.	V398
PHP	7.3.22	CVE-2016-7480	9.8	The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c in PHP before 7.0.12 does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.	V398
PHP	7.3.22	CVE-2016-3078	9.8	Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted	V398

				call to (1) getFromIndex or (2) getFromName in the ZipArchive class.	
PHP	7.3.22	CVE-2017-8923	9.8	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	V398
PHP	7.3.22	CVE-2016-4345	9.8	Integer overflow in the php_filter_encode_url function in ext/filter/sanitizing_filters.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.	V398
PHP	7.3.22	CVE-2016-4346	9.8	Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.	V398
PHP	7.3.22	CVE-2016-4344	9.8	Integer overflow in the xml_utf8_encode function in ext/xml/xml.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long argument to the utf8_encode function, leading	V398

				to a heap-based buffer overflow.	
PHP	7.3.22	CVE-2015-8080	7.5	Integer overflow in the getnum function in lua_struct.c in Redis 2.8.x before 2.8.24 and 3.0.x before 3.0.6 allows context-dependent attackers with permission to run Lua code in a Redis session to cause a denial of service (memory corruption and application crash) or possibly bypass intended sandbox restrictions via a large number, which triggers a stack-based buffer overflow.	V398
PHP	7.3.22	CVE-2017-7963	7.5	** DISPUTED ** The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of	V398
PHP	7.3.22	CVE-2010-4156	5.0	The mb_strcut function in Libmbfl 1.1.0, as used in PHP 5.3.x through 5.3.3, allows context-dependent attackers to obtain potentially	V398

				sensitive information via a large value of the third parameter (aka the length parameter).	
PCRE	8.44	CVE-2019-20454	7.5	An out-of-bounds read was discovered in PCRE before 10.34 when the pattern \X is JIT compiled and used to match specially crafted subjects in non-UTF mode. Applications that use PCRE to parse untrusted input may be vulnerable to this flaw, which would allow an attacker to crash the application. The flaw occurs in do_extuni_no_utf in pcre2_jit_compile.c.	V398
APACHE	2.4.46	CVE-2019-10098	6.1	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.	V398
APACHE	2.4.46	CVE-2019-10092	6.1	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.	V398

APACHE	2.4.46	CVE-2019-10097	7.2	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.	V398
APACHE	2.4.46	CVE-2019-10082	9.1	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.	V398
APACHE	2.4.46	CVE-2019-10098	6.1	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.	V398
APACHE	2.4.46	CVE-2020-1934	5.3	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.	V398
libjpeg	9d	CVE-2020-14152	7.1	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnobs.c in djpeg does not honor the max_memory_to_use setting, possibly causing excessive memory consumption.	V398
libjpeg	9d	CVE-2020-	7.1	In IJG JPEG (aka libjpeg)	V398

		14153		from version 8 through 9c, jdhuff.c has an out-of-bounds array read for certain table pointers.	
net-snmp	5.8	CVE-2019-20892	6.5	net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.	V398
Openssh	8.2p1	CVE-2019-6109	6.8	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.	V398
Openssh	8.2p1	CVE-2019-6110	6.8	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.	V398
Openssh	8.2p1	CVE-2019-6111	5.9	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses whi	V398

				ch files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirect	
Openssh	8.2p1	CVE-2020-12062	7.5	** DISPUTED ** The scp client in OpenSSH 8.2 in correctly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that	V398
Apache Portable Runtime	1.6.3	CVE-2017-12613	7.1	When apr_time_exp*() or apr_os_exp_time*() functions are invoked with an invalid month field value in Apache Portable Runtime APR 1.6.2 and prior, out of bounds memory may be accessed in converting this value to an apr_time_exp_t value, potentially revealing the contents of a different static heap value or resulting in program termination, and may represent an information	V276

				disclosure or denial of service vulnerability to applications which call these APR functions with unvalidated external input.	
Apache HTTP Server	2.4.27	CVE-2017-9788	9.1	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.	V262
Apache HTTP Server	2.4.27	CVE-2017-9789	7.5	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access memory after it has been freed, resulting in potentially erratic behaviour.	V262
SQLite	3.21.0	CVE-2016-6153	5.9	os_unix.c in SQLite before 3.13.0 improperly implements the temporary directory search algorithm, which might allow local users to obtain sensitive information, cause a denial of service (application crash), or have unspecified other impact by leveraging use of the current working directory for temporary files.	V262
SQLite	3.21.0	CVE-2017-10989	9.8	The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact.	V262
PHP		CVE-2017-	7.8	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before	V257

		11628		7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.	
--	--	-------	--	--	--