Precautions for updating iLO firmware

Thank you for purchasing our product. This document provides the precautions on the updating of iLO firmware. If you do not follow this document, a trouble, such as a start failure of the server, may occur. Read this instruction carefully, in order to prevent any error in the update operations. Furthermore, if the server malfunctions or the power is disconnected, due to blackout, thunder, disconnection, noise and other unexpected accidents during rewriting the data, in the worst case, damage occurs in the server and it does not work properly. In these cases, you might be responsible for paying for the repairs.

- Do not refresh the web browser screen by using the browser's reload button or pressing F5 key during updating the iLO FW. If you refresh the screen and the updating is unable to finish, reset the iLO.
- A TPM or TM is installed in this server. Before updating a system ROM or iLO firmware, suspend or back up any software that stores data on the TPM or TM. For example, if you use drive encryption software, suspend it before updating a firmware. Failure to follow these instructions might result in losing access to your data. Suspend software that uses TPM or TM before you update System ROM (BIOS) or iLO firmware.
- Reconfigure the SNMPv3 alert settings by using iLO web interface when updating from iLO firmware 1.10/1.15. Reconfigure the settings after updating when the server enables the SNMPv3 alert function.
- The SMTP Secure Connection (SSL/TLS) of AlertMail settings in iLO web interface is set to the enable when you update to this iLO firmware by this procedure. If you have enabled iLO AlertMail in previous iLO version, reconfigure AlertMail settings in accordance with your environment.
- You can restore the iLO settings backed up by iLO FW 1.20 but you cannot restore the other different version's backed up data. After operating this step, you need to configure the alert mail settings again because SMTP

Secure and SMTP auth settings are newly added in iLO FW 1.30. Backup and restore operations between different versions are not supported.

- To recover from losing iLO license key and iLO settings due to a hardware failure, we recommend that you back up the iLO settings by using the backup and restore function after updating iLO firmware.
- In addition to updating this iLO firmware, update the following firmware and software.
- System ROM (BIOS): Applying from Standard Program Package on Starter Pack
- Agentless Management Service: Applying from Standard Program Package on Starter Pack
- NEC ESMPRO ServerAgentService: Applying from **Applications** on Starter Pack
- Product Info Collection Utility: Applying from **Applications** on Starter Pack
- RESTful Interface Tool: Applying from **Applications** on Starter Pack
- NEC ESMPRO Manager: See "*Supplement to ESMPRO updating*".
- Express Report Service (MG) Receiving Information: See "*Supplement to ESMPRO updating*".
- When viewing the System Information tree in iLO 5 web interface, the Smart Array firmware displays a different version than the version in the Storage Information tab.
- About IPMI 2.0 RCMP+ Authentication Remote Password Hash Vulnerability (RAKP).

Perform any of the following:

- If you do not need to use IPMI, disable it. You can disable IPMI on iLO by using the Disable IPMI over LAN command. IPMI over LAN is disabled by default on iLO 5.
- Maintain the latest iLO firmware that contains the most recent security patches.
- Employ best practices in the management of the protocols and passwords on your systems and networks. Use strong passwords wherever possible.

  - If the IPMI must be used, use a separate management LAN or VLAN, Access Control Lists (ACLs), or VPN to limit and restrict access to your iLO management interfaces.

- If you try to update iLO firmware before OS installation、refer to OS installation guide and set [Date and Time]-[Time Format] of RBSU.

  And set the timezone so that [iLO Dedicated/ Shared Network Port]-[SNTP]-[Time Zone] corresponds to [Date and Time]-[Time Format] of EBSU after iLO firmware update.

  If [Time Format] is [Coordinated Universal Time (UTC)]:

  ->Set same timezone as [Time Zone] of RBSU(UTC equal to GMT).

  e.g.) If [Time Zone] is set to "UTC+09:00, Osaka, Sapporo, Tokyo, Soul, Yakutsk", select [Asia/Tokyo(GMT+09:00:00:00)].

  If [Time Format] is [Local Time]:

  ->Set the timezone to correspond to [Local Time].

  e.g.) If locale is Japan, select [Asia/Tokyo(GMT+09:00:00:00)].

- iLO 5 .NET Integrated Remote Console (IRC) does not launch from the Microsoft Edge 42 web browser. Perform any of the following:

  - Install a trusted certificate, and then enable the Integrated Remote Console Trust Setting located on the Remote Console & Media -> Security tab. This will prevent the redirection to HTTP and allow the .NET application to be trusted.

  - Click the "See all content" button from the blocked content menu to authorize untrusted content for the current session. The Microsoft Edge 42 web browser will then reload the window and allow the .NET integrated remote console to launch as in prior versions of the web browser.

  - Use Internet Explorer 11 to launch the .NET integrated remote console.

  - Use the standalone .NET console application.

- When the untrusted certificate warning pop-up window is displayed on iLO 5 web interface with the Microsoft Edge 42 web browser, perform either of the following:

    - Click the "Details" link on the popup window, and then click "Go on to the webpage" link to proceed. This will be required each time a help topic is opened in a pop-up window.
    - Use a different web browser that does not prompt to trust the sites untrusted certificate each time.
- Update to .NET Framework version 4.5.1 or later when you use iLO 5 .NET Integrated Remote Console (IRC) after installing this firmware.
- The remote console thumbnail in the iLO5 web interface may not be displayed on some systems with the Microsoft Edge 42 web browser. To view the remote console thumbnail, use the Internet Explorer 11 or another web browser (Firefox, Chrome mobile/Desktop) besides the Microsoft Edge 42 web browser.
- Peak server power in iLO5 web interface may exceed power supply capacity for short periods of time.
- Do not reset the iLO while POST is running. Invalid UUID or UUID (Logical) may be shown in overview page of iLO5 web interface.
- When you update iLO firmware to this version, there are cases in which 🛡 Risk will be displayed on the security dashboard page and the right upper part of iLO5 web interface. Address the risk according to your secure policy. Refer to *iLO5 user's guide* for more detailed information.

  The iLO security icon on the right upper portion of Web interface may be transparent even if “Overall Security Status” of [Security Dashboard] is “Risk”. "Overall Security Status" of [Security Dashboard] indicates the current security status.
- When you update iLO firmware to this version and iLO advanced license is installed, do not set “Downgrade Policy” to “Permanently disallow downgrades” in [Access Settings]-[Update Service]. Configuring this setting makes a permanent change to iLO. After you configure iLO to permanently disallow downgrades, you cannot reconfigure this setting through any iLO interface or utility. Setting iLO to the factory default settings will not reset this value.
- If you configured “Enabled” at [Access Settings]-[iLO]-[Require Host Authentication], the following symptoms will occur.

- Many “iLO detected more than 3 unauthorized login attempts.“ or “iLO RBSU login failure.” events are logged.
- An error will occur when you install Standard Program Package (SPP).

The following service and functionality do not work.

- RAID Report Service
- Reference to device and configuration information which are managed by iLO
- The system has System ROM version v2.00 or later and iLO5 firmware version 1.38 or earlier when system temperature is low, fans may rotate at high speeds. This occurs because the iLO5 firmware version 1.38 or earlier does not support the temperature sensors for PMem that is defined in the System ROM v2.00 or later.

Revision History

Dec 12 2024 iLO Firmware 3.10

ENHANCEMENTS:

- Support for Fan speed in terms of percentage from SNMP OID Get and Walk.
- Added cypher #17 support for iLO IPMI over LAN interface.
- Support for minimum 15 concurrent sessions per user for each interface.
- Fixes for specific SNMP OIDs for RDE capable storage controllers for controller, physical drive, and logical drive properties.
- Added IML alert and Redfish alert to report Intel Processor PROCHOT status.
    - Warning alert or an event when active PROCHOT longer than 60 seconds.
    - Repair alert or an event when nonactive PROCHOT status."
- Added support for iLO Two Factor Authentication with Active Directory Global Catalogs.
- Support for Windows Server 2025 operating system.
- Improved error messaging for iLO Two Factor Authentication.
- Added an option using REST API to rotate the ESKM password

FIXES:

- Fixed the offline firmware update failure through SPP and missing the inventory of hard drives.
- Fixed iLO upgrade issue due to file upload failure.
- Fixed a potential random server restart, or Uncorrectable Machine Check Exception (UMCE), when an iLO reset is triggered.
- Fixed an issue with the iLO Firmware auto recovery process.
- Fixed an issue where there was a communication loss between Ethernet 1Gb 4-port 331FLR adapter and iLO 5.
- Fixed an issue with the sensor index suffix in SNMP sensor name OIDs.
- Fixed an issue where, while updating the One Time Boot option to PXE boot device, the UEFI optimized boot mode was getting set to a disabled state.
- Fixed an issue with dynamic sensor number enumeration in IPMI response.
- Fixed an issue where LDAP mode used to get disabled due to version and size mismatch.
- Fixed an issue where HTTP calls to Rest server (through a web server) to create installset, initiate installset, and read installset was unstable leading to failure in BundleUpdate .

- Fixed an issue where data from Redfish when appended with available data, used to generate unexpected data.
- Fixed an issue query to memory URI response that got delayed or timed out.
- Fixed an issue for Embedded ALOM and for other cards where the indexes were automatically assigned.
- Fixed an issue where iLO reports a false error Duplicate IP address after resetting iLO.
- Fixed an issue where iLO Shared Network Port is unable to communicate with external routable devices.
- Fixed an issue where iLO may be unable to communicate with external routable devices after a power outage.
- Fixed an issue where DeviceDiscovery process failed to execute.
- Fixed an issue where an SNMP query on cpqHoMIBStatusArray status failed post upgrade to iLO 5 v3.00.
- Fixed an issue where the drives in the Embedded SATA controller were displayed in the label of Un-configured Drives instead of Drives.
- Fixed an issue where fetching the email ID for AD login users fails in a cross-domain setup, affecting the ability to send TFA tokens.
- Fixed an issue that involves a fallback mechanism to retrieve the email address from the parent domain if it cannot be fetched from the cross-domain.
- Fixed an issue where fetching the email details of an LDAP user where DistinguishedName containing special characters were causing the two-factor authentication process to fail.
- Fixed an issue where the hpsetup/secureflash engine reports the iLO 5 firmware update as a failure.
- Fixed the cpqHoMIBStatusArray status issue that did not get updated with proper details when a drive attached to Smart Array P408i-a SR controller failed or degraded.
- Fixed an incorrect AMS status (Not Available) that appeared on the iLO interfaces while operating system indicated AMS status as running.
- Fixed an issue where the MCTP retry mechanism in i2c communication failed.
- Fixed an issue where the IPMI boot parameters were not functioning through the BMC IPMI interface.
- Fixed an issue where the Kerberos client advertised insecure encryption (RC4, DES) types and rejected the deprecated ones. As a part of this fix, RC4, DES, and 3DES algorithms are removed from the Kerberos requests.

- Fixed an issue of firmware update failures by increasing the time delay between retries for PCIe VDM transmit buffer.
- Fixed an issue for the sensor values that were reported in the GET_SENSOR response though these sensors were marked as non-supported in the PDR table.
- Fixed the issue with missing storage controller condition values with the IDA condition for the MIB status array for the SR and MR Controller of Smart Array.
- Fixed an issue of abnormal noise in the fans of the several server models during POST across newer iLO 5 firmware versions.

Apr 17 2024 iLO Firmware 3.04

ENHANCEMENTS:

- Configuration to allow disabling/enabling all weak ciphers and key lengths for SSH and TLS interfaces in Production security mode
- Storage Page enhanced to display storage enclosure, switch and port information in the topology
- Support for TLS v1.3
- Support for consistent URIs (indexes) under Ethernet interfaces for systems in Gen 10 servers at all times.
- Ability to switch from DHCP6 to static IPv6 address for the same IP address.

FIXES:

- Fix for incorrect temperature sensor values and sensor indices reported by iLO SNMP interface
- Fix for inconsistent physical drive status reported by iLO SNMP interface as compared with iLO GUI or Redfish interfaces
- Support added for sending iLO AlertMail with TLS enabled, in conformance with RFC3207
- Fix for configuring one time boot options via in-band and out-of-band IPMI methods
- Fix for Web User interface being rendered inaccessible after the storage tab is clicked, in a server with large number of drives
- Fixed incorrect messaging when FW update failed with BundleUpdateComponent download failure
- Fixed bundle update status reporting when Component download fails after all retries done.

- Fixed an issue where there was a communication loss between HPE Ethernet 1Gb 4-port 331FLR adapter and HPE iLO 5.
- Fixed an issue of invalid values for SNMP OIDs during SNMPWALK.
- Fixed an issue where SMBIOS data file present in NAND is removed and recreated every time a server reboots.
- Fixed an issue where physical drive status was reported incorrectly in SNMP.

Dec 14 2023 iLO Firmware 3.00

ENHANCEMENTS:

- OpenSSL v1.0.2 in iLO FW is patched with Extended Master Secret support for TLS1.2
- SNMP GET, GET-NEXT and WALK support added for the following storage controllers on iLO5
  - HPE MR216i-a Gen10 Plus
  - HPE MR216i-p Gen10 Plus
  - HPE MR416i-a Gen10 Plus
  - HPE MR416i-p Gen10 Plus
  - HPE SR932i-p Gen10 Plus
  - HPE SR416i-a Gen10 Plus
  - HPE NS204i-p Gen10 Plus Boot Controller"
- Updated the Eventing mechanism for State Transitions for Security Parameters for Security Dashboard
- Redfish includes direct attach backplane in Fabric collection
- Redfish schema amendments for DMTF compliance
- Gracefully handle multiple boot to UEFI commands in installset
- Provide update statistics via Redfish for firmware bundle update
- Redfish includes direct attach backplane in chassis collection
- Redfish includes downstream backplane in chassis collection
- Providing granular control on Security Parameters present on Security Dashboard
- Added Enable/Disable of User Accounts option from Redfish and iLO GUI
- For PLDM components, added the ability to selectively update the target devices on the system from Install sets and Update task queue
- iLO needs to provide IPv4 address for RDE enabled NIC
- Support for telemetry streaming using Redfish event subscription

- Added capability in iLO for Two Factor Authentication using OTP (One Time Password) for Microsoft AD users
- To display drive enclosure info in Firmware tab in iLO
- Support for controller which goes for functional reset runtime
- iLO to mark the correct component update status for runtime agent updatable components based on the update status and update result
- Secure erase of data based on the usecase (customer, factory or openbmc ownership transfer)
- iLO stops the bundle update in the scenario where BootToUefi task goes to exception to ensure Graceful shutdown of server
- iLO Support for OBSE in factory mode without the need for Advance License
- Added support for comma (",") as a delimiter for multiple email IDs in AlertMail feature

FIXES:

- Slowness due to continuously polling on timer expiry leading to increased CPU utilization
- Added timestamp register call before iLO starts VSP logging to file to fix iLO VSP locks-up after an iLO reset if there is output displayed during the iLO reset
- Firmware update fails through iLO web interface due to loss of network connectivity to iLO. You can now retry after 5 minutes when the network connectivity with iLO is restored
- Fix has been implemented to show right data in redfish, which includes to suppress additional SetObject name when adapter provides expanded data for GET operation in RDE
- Excessive event issue is fixed when RDE and DCi coexist on the system on iLO 5 and iLO 6
- Increased the maximum boot order to 512 as specified by UEFI EV specification
- UefiDevicePath length increased from 256 bytes to 1024 bytes.
- Incorrect sensor values for some sub-components in IPMI response.
- Enforced a limit of 14 bytes for DHCP v4 clientId. An error response of "400 - Bad Request" will be observed if the length is beyond 14 characters.
- Incorrect reporting of the firmware version of Intel NVMe drives
- iLO Two-Factor authentication login fails when AD user login name is used as username for iLO Login instead of AD user display name
- Incorrect reporting of the Nic card port status from IPMI SDR list

- OEM iLO component does not show the OEM equivalent entry for Intelligent Provision in One Time Boot Option
- Handling delayed device discovered in UEFI mode during discovery phase
- Persist the KCS interface setting across iLO reboots
- Capability to enable KCS interface setting without needing a factory reset

May 11 2023 iLO Firmware 2.90

ENHANCEMENTS:

- Support for import of a trusted SSL certificate and its corresponding private key.
- Inclusion of Context property in Redfish event which will display the value set by user during Redfish event subscription creation.
- Supporting new iLO ASIC motherboard.
- Handle Devices reconnection when Bus Device Function information has changed after the Device comes back after Reset.
- Handle Type - A Firmware Update gracefully even when iLO goes for a reboot.
- Enable/disable SNMP v1 and v3 independently

FIXES:

- When you reset the server after SAN boot configuration (enable ports, and configure WWPN), SAN boot may fail because the settings as for SAN boot is clear to defaults by the Fibre channel card.
- Not clearing error in processing interrupts can lead to interrupt storms leading to firmware watchdog reset
- NVMe drive reporting invalid drive IML and illuminating the Amber LED
- In a configuration with more than 10 logical network controller on bringing the logical controller up or down data doesnt get updated and AMS banner ; iLO did not detect Agentless Management…” shows up in iLO GUI.
- UEFI iLO config utility lets users add special characters to the ILO hostname
- iLO IP addresses were not included in the SSL certificate SAN even when the user selects this option in the UI
- iLO is not holding onto Redfish Subscriptions due to invalid Sender-Address in Redfish Event Header
- For URI /redfish/v1/Managers/@ManagersId/SecurityService/, PATCH on the property TLSVersion using “Enabled” or ”Disabled” fails.

- RDE Changes to create Location URI for newly created resource when LRT is completed
- RDE client MC error code mapping is wrong
- iLO FW Communication Issue: iLO cannot be accessed via Web UI
- Server fails to power up as secure start did not complete successfully
- Discrepancy observed in the Current Operating Power comsumption data
- Incorrect CPU throttling information observed in iLO.
- iLO incorrectly reports missing PSUs and sensor readings.
- System shuts down when updating EXPRESSBUILDER and SPP.
- Issues observed on iLO with Express5800/R120h-1M Server and NVMe SSD Boot drives combination.
- Thermal policy is not spinning up fans in some cases resulting in inadequate air flow.
- Local User Passwords containing a backslash character may not be set correctly in the iLO 5 Command Line Interface
- Organizational Unit attribute is mandatory for the iLO Redfish REST API for generating a CSR whereas in the UI it is marked Optional.
- Automatic Certificate Enrollment may not work if the Certificate Authority signing the iLO Certificate Signing Request is an Intermediate.
- Trap Source Identifier setting periodically changes to iLO Hostname from previously defined OS Hostname
- IE not updating due to incorrect Target GUID

Sep 14 2022 iLO Firmware 2.72

ENHANCEMENTS:

- Added support to auto-restore the IPMI and SNMP configuration settings to custom defaults (manually enabled by the user) instead of the factory defaults during abrupt AC power cycle.
- iLO PLDM Downstream Drive firmware update support enabled.
- Enhanced the Alerting Mechanism to allow clearing of Events without resetting iLO.
- PATCH support for Redfish Property “DateTimeLocalOffset”.
- Ability to disable/enable TLS 1.0 and/or TLS 1.1 in Production state.
- The Temperature page now displays the temperature details of the available PCIe subcomponents.

FIXES:

- ‘SessionTimeout’ property missing under &lsquoredfish/v1/SessionService’ URI
- GUI reporting configured drives as unconfigured.
- A router failover post iLO NIC link down and link up could cause iLO to be rendered unreachable over router (default gateway).
- Incorrect SNMP Trap Data value for cpqSm2CntlrBadLoginAttempts (OID 1.3.6.1.4.1.232.9.2.2.14)
- Patch operation under redfish URI chassis/1/Thermal not working
- When a storage controller is configured in Passthrough Mode in ESXi, iLO might take a bit longer to discover Direct Attach NVMe Drive.
- iLO hostname displays the previous host name after iLO reset.
- NVMe Backplane Firmware Package 1.0 is not getting updated through iLO.
- The following weak TLS 1.2 ciphers are disabled in High security state:
    - 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
    - 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
    - 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
    - 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256

July 28 2022 iLO Firmware 2.71

FIXES:

- Port Status of 331i & 562FLR Network Adapter cards do not change from “unknown” to “ok” in rare occasions.
- “show swid” command displays P408i-a SR card twice.
- iLO responds with wrong Network port information during Ports collection and Network Device Functions collection.
- Server boot gets stuck on POST while loading Encryption keys for secure boot.
- EID Table information is retained in AHS though MCTP discovery is disabled.
- Front Display Port (DP) on Universal Media bay does not work in certain instances.
- iLO unable to authenticate users intermittently when directory authentication is enabled.

ENHANCEMENTS:

- UBM6 Backplane Detection Support : New backplane basic support added without firmware update support.

Feb 23 2022 iLO Firmware 2.65

FIXES:

- Deployment needs to be run twice to reflect Firmware baseline successfully.
- Change in response of Redfish API causes Oneview not to fully discover the Port Map Information.
- RF subscription gets exhausted in certain situations.
- iLO not able to auto recover when an IML corruption happens.
- Adapter Virtualization Mode not persistent across reboots.
- ipmitool lists incorrect number of network port links.
- Fixed the following issues occurred when the iLO version is 2.60 or lower and the host OS is Red Hat Enterprise Linux.
    - SNMP alerts were not sent when a failure occurred or when "Send test alert" is executed
    - The following log is logged so manytimes in SYSLOG
      "smad[XXX]: [ERR]: Timeout for receiving OPEN_PDU after socket connected"

ENHANCEMENTS:

- Validation of LDAPv3 based authentication using OpenLDAP based directory server.
- Added Support for RDE Read and Write operations.
- Added Support for Firmware update using Common PLDM based Package for Direct Attached UBMs (1/2/3/4).

Dec 06 2021 iLO Firmware 2.60

FIXES:

- Fixed an issue where Network Tab page in iLO GUI doesn’t refresh automatically post Server Reset.
- "StructuredName" Redfish Property is hidden when the value of this field is an empty string.
- Fixed an issue where iLO may become inaccessible after consecutive setting of factory defaults.
- Improved power supply information reporting on Edgeline servers.
- Intelligent Provisioning not accessible after a rare server reboot.

ENHANCEMENTS:

- Support for Automatic SSL Certificate Enrollment using Simple Certificate Enrollment Protocol.
- Addition of DIMM Manufacture date in RedFISH output of Memory Resource.
- Added monitoring of User-defined temperature threshold for PCI Zone sensors on Edgeline servers.

Oct 1 2021 iLO Firmware 2.55

FIXES:

- Fixed an issue where the Adapter Virtualization Mode was not persistent across reboots.
- During System boot/reboot, iLO will stall the complete storage controller discovery such that encryption status query happens after PCIeVDM interface is ready.
- Fixed an issue where none of the Controller were getting detected when Encryption was Enabled.
- Fixed intermittent issue where none of the NVME drives were getting detected in OS when iLO is reset multiple times.
- Fixed a configuration sync issue during IPv6 initialization when SLAAC Enable/Disable settings were modified.

- Support added to increase the mapping limit of 32 to 64 physical drives to one logical drive.
- Fixed the long boot time issue when encryption is enabled on smart array controller.
- Fixed the NS204i-p unknown status issue after the windows reboot.

ENHANCEMENTS:

- Support import of SSL certificate which is more than 20KB via iLO REST and GUI.
- Support for 64 Character length Password similar to how other vendors provide.
- Implemented workaround for health monitoring of NVME M.2 drives as these were partially compliant to NVMe-MI spec.

May 07 2021 iLO Firmware 2.44

FIXES:

- Fixed the followings potential security vulnerability

CVE-2021-29201 - XSS

CVE-2021-29204 - XSS

CVE-2021-29205 - XSS

CVE-2021-29206 - XSS

CVE-2021-29207 - XSS

CVE-2021-29211 - XSS

CVE-2021-29202 - local buffer overflow

CVE-2021-29208 - DOM XSS, CRLF injection

CVE-2021-29209 - DOM XSS, CRLF injection

CVE-2021-29210 - DOM XSS, CRLF injection

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2021-29201	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29202	CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:L/A:L	6.4	(AV:L/AC:H/Au:M/C:C/I:C/A:C)	5.9
CVE-2021-29204	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29205	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29206	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29207	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2
CVE-2021-29208	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H	7.6	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1
CVE-2021-29209	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H	7.6	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1
CVE-2021-29210	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H	7.6	(AV:N/AC:H/Au:S/C:C/I:C/A:C)	7.1
CVE-2021-29211	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L	3.1	(AV:N/AC:H/Au:M/C:N/I:P/A:P)	3.2

March 08 2021 iLO Firmware 2.41

ENHANCEMENTS:

- Added IPMI lan6 commands support
- Added ability to view DIMM serial numbers through iLO GUI and redfish API
- iLO Security logs are now listed in Operating System logs
- Added ability to change serial Interface configuration using standard redfish schema
- Added iLO hostname as part of redfish event header
- Power meter data shown in GUI and IPMI CLI has been extended for 1 week
- Enhanced to avoid BMC reset during system POST
- Option to delete LDAP CA certificate and import CA Certificate of public key larger than 4096 bits (8192 bits, 16352 bits)
- Banner to be displayed at the SSH login
- iLO GUI to display the Host Operating System Version
- Display platform Resiliency and Serviceability (RAS) policy in iLO GUI
- Added standard redfish schema support for Computer System – Reset, Graceful restart actions
- Real CPU temperature is reported in addition to normalized temperature
- Ability to control LED for locating direct attached SATA drives
- Ability to reset power for direct attached SATA drives

FIXES:

- Fixed potential security vulnerability CVE-2020-27337 in network stack

Reference	V3 Vector	V3 Base Score	V2 Vector	V2 Base Score
CVE-2020-27337	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	7.3	(AV:N/AC:L/Au:N/C:P/I:P/A:P)	7.5

- Error when a user with Read-only role tries to change the password of own account.
- Resetting iLO to default security state i.e. ‘Production’ via hponcfg /reset command fails when iLO is in ‘High Security’ state and ‘Require Host Authentication’ (RHA) is disabled.
- Continuous logging to IML of a CHIF Error running ESXi with iLO 5 v1.46
- Random messages "smad[]: No response from iLO for Hello" seen in certain Operating Systems
- Copy/paste may not work for more than 255 characters to VSP terminal in Linux platforms

- Fixed the issue that the system may not power on with iLO 5 Firmware v2.35 (or Earlier) in extremely rare instances

Oct 13 2020 iLO Firmware 2.31

ENHANCEMENTS:

- MCTP now addresses the iLO false alarm "device/adapter not responsive" issue.
- Shutdown by virtual button press is included in the iLO enhanced reset cause.
- Support for initiating the One-button secure erase process from the iLO web interface Lifecycle Management - Decommission page.
- User account roles provide predefined privilege sets or allow you to define a custom set.
- New HTML5 remote console modes: Standalone mode and New Window mode.
- Configuration of Minimum Fan speed using iLO interfaces.
- Users can view and modify the System thermal configuration settings using iLO interfaces.
- New REST alerts for Auto Heal and Safe Mode.
- Enabled the iLO webserver to identify the source of request as Host over Virtual NIC.
- When iLO is set to the factory default settings, Virtual NIC is disabled by default.
- Ability to read DIMM serial number using REST API
- When iLO is set to the factory default settings, Virtual NIC is disabled by default.

FIXES:

- Zero Sign In login fails when Kerberos authentication is configured for a large number of groups.
- When Using Redundant Gateways That Use Gratuitous Address Resolution Protocol (ARP) When Failing Over, iLO 5 May Not Be Reachable by Some Network Clients After a Fail Over
- Remote Syslog is made to adhere to RFC 5424 for Unstructured data format
- On VSP performing ‘cat’ or ‘head’ or 'tail' command on a file that contains some embedded NULL characters hangs the VSP or trims the file after the NULL character

Jun 22 2020 iLO Firmware 2.18

The following issues have been fixed in iLO 5 2.18:
FIXES:

- Ripple20 vulnerabilities might affect the TCP/IP stack.

Feb 11 2020 iLO Firmware 2.14

ENHANCEMENTS:

The following enhancements are part of iLO 5 2.14:

- Support new Accelerators:
  - Xilinx Alveo U250
  - Xilinx Alveo U50
- User can now define pre-caution threshold alert value for the inlet ambient sensor by RESTful API interface.

Oct 30 2019 iLO Firmware 2.10

ENHANCEMENTS:

The following enhancements are part of iLO 5 2.10:

- Added a security log that lists security events recorded by the iLO firmware.
- Supports Firmware Verification functionality at [Administration]-[Firmware Verification].
- Extended Secure Start to verify CPLD on Gen10 Plus servers.
- Updated menu path and feature names for the Performance Management features. The features that were accessed through the Intelligent System Tuning menu can now be accessed through the Performance menu.
- New alert for recovery events.
- SUM/SUT support on servers using the High Security, FIPS, or CNSA security states.
- Support for staging firmware to update direct-attached hard drives through the UEFI System Utilities.
- Ability to import and export drive bay mapping information.
- Daily firmware flash limit, to protect iLO, ROM, and CPLD from repeated flashing attacks.
- Performance data logging in a new Active Health System record.
- Increased the certificate size limit from 4096 to 8096.
- When iLO is set to the factory default settings, Virtual NIC is enabled by default.
- The following System Diagnostics features are supported on Gen10 Plus servers:
  - Booting to safe mode—Allows you to boot the server with a safe minimum configuration.
  - Booting to intelligent diagnostics mode—Allows the system to automatically diagnose a boot failure during POST.

  - Restoring the default manufacturing settings—Resets all BIOS configuration settings to their default manufacturing values. This process deletes all UEFI nonvolatile variables, such as boot configuration, Secure Boot security keys (if Secure Boot is enabled), and configured date and time settings.
  - Restoring the default system settings—Resets all BIOS configuration settings to their default values and restarts the server. This option preserves some UEFI settings.
- Modified the text of the iLO time zone selections to match the system ROM time zone selections. For backward compatibility, you can use the previous time zone selection text or use the new text in APIs to set the time zone.

FIXES:

The following issues have been fixed in iLO 5 2.10:

- System GPUs might be listed without GPU version information.
- Incorrect power consumption information is displayed in RIBCL output and the Active Health System Log.
- If the domain name system is unavailable, an HPE ProLiant Gen10 Server might stop responding for up to three minutes during startup.

Oct 14, 2019 iLO Firmware 1.47

FIXES:

- Fixed a problem which iLO time goes back, when iLO reset was executed in the condition that OS has been running over 49.5 days from the last OS reboot.

Jun 27, 2019 iLO Firmware 1.45

FIXES:

- Fixed problem introduced in iLO 5 v1.43 which could cause an HTTP connection to be refused under high activity of REST calls.

May 23, 2019 iLO Firmware 1.43

FIXES:

- Fix for potential firmware use of system memory after free, which could lead to an OS exception or memory corruption under Linux or ESX when using hpilo driver. It was not an issue for Windows.
- Fix so iLO 5 can connect to switch when both are set to 100 Full Duplex.

- Fixed REST call so that "ilorest -d serverlogs --selectlog=IML --clearlog rc 255" does not fail when it should succeed.
- Fixed problem with erroneously logging IML events like the following for "exceeding power capacity threshold" when it should not be logged.

  e.g.: Server power: %1W exceeded power capacity threshold %2W

  *The IML logs in question will look like one of the following, where %1 is an average power reading and %2 is a threshold equal to 10% above the total or redundant power supply capacity.
- In only Express5800/R120h-2M, fixed a problem that Backup and Restore option in iLO 5 may fail to complete when a server is fully populated with eight PCI cards.

ENHANCEMENTS:

- Added VLAN tagging support on iLO Dedicated NIC.
- Enhanced SNMP functionality to generate the iLO SNMP EngineID automatically after iLO resets.Reduced the number of Redfish resource change events sent. Removed watching of fields that change frequently.
- BIOS Admin password will NOT cause iLO to act as if Require Host Authentication is Enabled.

Feb 05, 2019 iLO Firmware 1.40

Fixes:

- User interface fixes and improvements.
- Fixed an issue where power supply status changes may be delayed.
- Device Inventory could display a parse error under Internet Explorer 11 when certain PCI Cards are installed.
- Improved shared network port out-of-band LOM resuscitation to reduce the scope and the frequency of system power-on/power-off during systems shutdown/reboot.
- iLO communication issues in certain configurations where a server is set to Auto-Power-On after an AC power cycle.
- Fixed issue where pressing UID button can occasionally cause server to power off
- Fix for "VGA Port Detect Override" to show video in all cases where monitors are installed.
- Fix for intermittent file upload failures.
- Fix for issues with Virtual Media in FIPS mode.
- Fix for issues with simultaneous use of virtual DVD and floppy in FIPS mode.
- Fix for USB floppy when used with ESXi 7 installation driver.
- Fix for erroneous reporting of disk drive overheating.
- Fix for potential RESTful API errors at boot with multiple NICs installed.

- Fix to add iLO 5 NIC information into anonymous XML response.
- Fixed false errors showing link lost on NICs when link never seen in IPMI.
- Fixed an issue where PCIe cards such as RAID card status may be “Unknown” in Device Inventory or “Strage Information” may be not shown in Strage page after server reboot.

Enhancements:

- Ability to edit Maintenance Windows in Firmware & OS Software section
- Added Password Complexity feature to Security > Access Settings
- Enable/disable for overlay video showing Server Health Summary
- Downgrade Policy - Specifies how iLO handles requests to downgrade any of the firmware types that you can update through iLO.
- Virtual NIC functionality (disabled by default)
- Enabled One-button Secure Erase via Express Builder
- LDAP/Directory settings configurable via Redfish
- Security Dashboard - displays the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features.
- Support for Gemalto SafeNet and SafeNet AT key managers
- Show NVMe wear level
- Ability to edit Maintenance Windows in Firmware & OS Software section
- Ability to backup and to restore a copy of the iLO configuration settings to/from iLO non-volatile memory via REST calls.
- Added Downgrade Policy setting to Security->Access Settings page.
- New features under the Intelligent System Tuning menu:
    - Performance Monitoring—View performance data collected from supported sensors on servers with Innovation Engine support. You can configure alerts based on the collected data.
    - Workload Performance Advisor—View selected server workload characteristics. You can view and configure recommended performance tuning settings based on the monitored data.
- Enhanced management for the embedded 4 GB non-volatile flash memory (also known as the NAND).

Security Fixes:

- Local Bypass of Security Restrictions (CVE-2018-7113)
- Remote Cross-Site Scripting in iLO 5 web interface(CVE-2018-7117)
- Cross-Site Scripting (XSS)(CVE-2019-11982)
- Buffer overflow in CLI(CVE-2019-11983)

CVE-ID	V3	V2

	Vector	Basic Score	Vector	Basic Score
CVE-2018-7113	AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L	6.4 (Medium)	(AV:L/AC:L/Au:N/C:C/I:C/A:P)	6.8 (Medium)
CVE-2018-7117	AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H	7.6(High)	(AV:A/AC:L/Au:S/C:P/I:C/A:C)	7.4(High)
CVE-2019-11982	AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H	8.3(High)	(AV:N/AC:H/Au:N/C:C/I:C/A:C)	7.6(High)
CVE-2019-11983	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H	7.0(High)	(AV:N/AC:M/Au:N/C:P/I:P/A:C)	8.3(High)

Sep 11, 2018 iLO Firmware 1.38

- Fix the issue that the OS panic or OS stall may be happen in Linux or VMware.

Aug 14, 2018 iLO Firmware 1.35

- Fix for improper Smart Array error reported: Cache module board backup power failed.
- Fixed where iLO5 may become unresponsive after ejecting virtual media.
- Changed the design of the icons that indicate privilege level of user or group in web interface.

This version adds support for the following features and enhancements:

- VGA Port Detect Override--Controls how devices connected to the system video port are detected. Dynamic detection protects the system from abnormal port voltages. This setting is enabled by default, and can be used for troubleshooting cases when there is no video output to displays, KVM concentrators, or active dongles.
- DHCP Client ID override via iLO5 RESTful API.
- Modified the following security vulnerability.
  - ➢ Remote execution of arbitrary code, Local Disclosure of Sensitive Information(CVE-2018-7105)

CVE-ID	V3		V2	
	Vector	Basic Score	Vector	Basic Score
CVE-2018-7105	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2(High)	(AV:N/AC:L/Au:S/C:C/I:C/A:C)	9.0(Critical)

May 31, 2018 iLO Firmware 1.30

- When you use iLO Virtual Media to install an operating system, installation might fail when iLO is configured to use the Shared Network Port.
- In rare cases, a server runs out of available SSH sessions because the sessions are not reclaimed when a client disconnects.

- iLO 5 unexpectedly restored itself to the factory default settings when a user did not initiate the process.
- When Auto Power-On is set to Always Power On or Restore Last Power State, the server might not power on after a cold reset.
- NVMe drive model numbers are incorrect or inconsistent.
- Added support for RSA-PSS certificate signatures.
- If ”Web Server Non-SSL Port” is set to value except for the default port number, EXPRESSBUILDER is not launched.
- If ”Web Server Non-SSL Port” is set to value except for the default port number, JAVA IRC is not launched.
- When the same time zone is set between BIOS and iLO, the system time will be incorrect time.
- iLO cannot display Express5800/R120h-1M and R120h-2M standard network adapter(Ethernet 1Gb 4-port 331i) MAC address.

- The significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.
- Improved HTML5 IRC performance, including:
  - ➢ Added virtual keys to improve the ability to send keyboard actions to the server.
  - ➢ Added the ability to configure the keyboard layout in the HTML5 IRC
  - ➢ Added Virtual Media support for local ISO and IMG files.
- Firmware and software update enhancements:
  - ➢ iLO users can now view, create, and delete maintenance windows.
  - ➢ A new check box allows users to clear the installation queue when initiating an install set.
  - ➢ Updated the iLO RESTful API and iLO web interface to report when a reboot is required after an installation task completes.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored.
- AlertMail now supports SSL (TLS) for secure email.
- AlertMail now supports external SMTP mail servers.
- Added an SNMP trap for when all host NICs are down.
- Updated to OpenSSL-1.0.2u-fips-2.0.16.
- Added the list of open source licenses to the login page.
- Added Intelligent System Tuning features to the iLO web interface. From the iLO web interface, you can view the configured settings, configure Jitter Smoothing, and launch Intelligent Provisioning to configure Workload Matching and Core Boosting.

- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove an SSL certificate and regenerate the iLO self-signed certificate.
- Modified the following security vulnerability.
  - Remote or Local Code Execution(CVE-2018-7078)
  - Remote: Denial of Service (DoS)(CVE-2018-7101)

CVE-ID	V3		V2	
	Vector	Basic Score	Vector	Basic Score
CVE-2018-7078	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	7.2(High)	(AV:N/AC:L/Au:S/C:C/I:C/A:C)	9.0(Critical)
CVE-2018-7101	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5(High)	(AV:N/AC:M/Au:N/C:N/I:N/A:C)	7.1(High)

Feb 2, 2018 iLO Firmware 1.20

- Support for HTML5 Integrated Remote Console (IRC) in English keyboard environment.
- Support for a mouse wheel in Integrated Remote Console (IRC).
- Support for IPv6 on Shared Network Port.
- Support for iLO Federation on Shared Network Port.
- Support for importing SSL certificates of the RSA-PSS algorithm.
- Support for SNMPv3 Inform notification.
- Enhanced SNMP alert function, which enables to select any of SNMPv1 Trap, SNMPv3 Trap, and SNMPv3 Inform, for each alert destination.
- Enhanced SNMP alert function, which enables to configure the engine ID for each SNMPv3 user.
- The maximum number of the registerable alert destinations increased to 8.
- The maximum number of the registerable SNMPv3 users increased to 8.
- Support for periodic HAS Trap function.
- Support for new “Add to Queue” pane on enhanced firmware and software update page.
- Support for “Remove All” option on enhanced firmware and software update page.
- Support for “Update Recovery Set” option on enhanced firmware and software update page.

- Support for the function to display the names of software installed in OS and/or running software in Japanese on Web interface. (Agentless Management Service needs to be updated.)
- Support for properties of NVMe drive on RESTful API.
- Support for device inventory on RESTful API.
- Support for Service Account option to distinguish iLO user accounts used in management software and the like.
- Change the IML event recorded when the status of system LAN is changed.
- Improved the problem that the System ROM (BIOS) version is missing in AlertMail messages.
- Improved the problem that Virtual Media devices are inaccessible when two virtual devices are mounted simultaneously.
- Improved the problem that a floppy image connected through a script virtual media is always mounted read-only.
- Improved the problem that the alert is not always issued in case FQDN is specified in the address of the remote Syslog server.
- Improved the problem that the alert is not always issued in case FQDN is specified in the SMTP server and the IPv6 address is returned when the name is resolved.

Aug 17, 2017 iLO Firmware 1.15

- Support for the functions to backup and restore the iLO configuration.
- Support for diffie-hellman-group-exchange-sha256 as SSH Key Exchange authentication method.
- Support for multiple destination AlertMail email addresses. Enter the addresses separated by a semicolon.
- Support for Power Cycle on RESTful API.
- Support for properties of High Efficiency Mode on RESTful API.
- Support for properties of Cache Module Serial Number on RESTful API.
- Support for properties of Login Security Banner on RESTful API.
- Support for properties of Current Power On Time on RESTful API. (Provides the time since the system was last powered on.)
- Support for properties of Persistent Mouse/Keyboard Enabled on RESTful API.
- Support for properties of current Cipher Suite on RESTful API.
- Support for propagate NTP Time to Host function to transfer the time which iLO obtained from SNTP server to the host, at the first POST after turning AC to ON.

- Improved the problem that the iLO web interface intermittently displays incorrect memory status after a system reset.
- Improved the problem that the server power page stalls when loading the server power information.
- Improved the problem that Virtual Media status is not displayed in the Java IRC.
- Improved the problem that the local client keyboard might get disabled when the Java IRC is in use.
- Improved the problem that the maximum available power is displayed incorrectly.
- Improved the problem that the first attempt to clear IML fails if the IML contains a maintenance note.
- Improved the problem that secure boot cannot be configured through the RESTful API, even if the pending configuration is in UEFI mode.
- Improved the problem that Onetimeboot and Continuousboot do not take effect in RESTful API.
- Improved the problem that an iLO web interface error occurs after an installed SSL certificate was deleted by using the RESTful API.
- Improved the problem that an iLO Federation authentication error might occur when group names with unsupported characters are used in URLs without correct encoding.
- Improved the problem that a false positive “Insecure Cache Management Policy” issue is reported by some security scanners.
- Improved the problem that iLO federation group cannot be created by the one or two-byte group key.

Jun 7, 2017 iLO Firmware 1.10

- Initial release.