BIOS Version 2.18.1 for Dell PowerEdge R440, R540, and T440 Servers

Release Notes

DELL Technologies

Release Notes

BIOS

Basic Input / Output System (BIOS) facilitates the hardware initialization process and transitions control to the Operating System (OS).

Current version

2.18.1

Release date

February 2023

Previous version

2.17.1

Release summary

This release highlights the Intel Purley Refresh IPU 2023.2 Reference Code version 627P11. For more information about specific items added and resolved in this BIOS version, see the **Fixes** and **New and enhanced features** sections.

Priority and recommendations

Urgent—Dell highly recommends applying this update as soon as possible. The update contains changes to improve the reliability and availability of your Dell system.

Supported devices and platforms

The PowerEdge R440, R540, and T440 servers.

Fixes

Fixed an issue where the system stops unexpectedly (at a black screen that says, “Booting from Virtual Optical Drive.”) while using a virtual optical drive to install Red Hat Enterprise Linux (RHEL) version 8.7 or version 9.1.

New and enhanced features

- Updated the following:
  - Processor and Memory Reference Code for the second-generation Intel Xeon Processor Scalable Family to IPU 2023.2.
  - The Integrate Intel Purley Refresh PV Candidate Reference Code Version to 627P11.
  - Processor Microcode to version 0x3501 for the second-generation Intel Xeon Processor Scalable Family.
  - Processor Microcode to version 0x6F05 for Intel Xeon Processor Scalable Family
  - S140 Software RAID firmware to version 5.9.0-0000.
  - Added option for enabling/disabling if prompt on iSCSI connection error in iSCSI Device Setting (Default is enabled).
  - This product release contains security updates. Once available, information will be accessible on the *Dell Security Advisories and Notices* website.

Known issues

None for this release.

Important notes

- Rolling back to a previous BIOS from 2.14.2 will cause a TXT trusted boot failure with TXT enabled. Since the Intel ACM’s SVN (Security Version Number) was increased in BIOS 2.14.2 to address the Security Vulnerabilities CVE-2021-0559, CVE-2021-33123, CVE-2021-33124. The purpose of incrementing the SVN is to prevent executing an older ACM with the vulnerabilities.

- The INTEL ACM's SVN was also increased in the BIOS 2.9.4 since the 1st BIOS revision of this platform as well.

- When using an Update Package (DUP) file or the UEFI Shell command (an EFI file) to update the BIOS version, the process takes longer duration. To resolve this issue, do one of the following:
  - Update the BIOS version using an Out-of-Band (OoB) tool such as iDRAC—use GUI or run the RACADM command. See the iDRAC User's Guide or RACADM CLI Reference Guide available on the support site.
  - Reduce the system memory capacity by physically removing the memory modules and perform the BIOS update and retry the operation.
- When one or more PCIe devices are installed on the system and if the cards require more of limited legacy I/O resources, the system might modify the I/O resources causing it to restart automatically. The UEFI0256 error message is logged, and the system does not allocate the PCIe resources required. To resolve this issue, do one of the following:
  - Remove the PCIe cards from the system that are not used to free up the legacy I/O allocation and provide more I/O allocation space.
  - From the **System Setup** menu, disable to PCIe cards that are not used to free up the legacy I/O allocation.
- When one or more PCIe devices are installed on the system and if the cards require more of Memory-Mapped I/O (MMIO) resources, the system might modify the MMIO resources causing it to restart automatically. The UEFI0256 error message is logged, and the system does not allocate the required PCIe resources required. To resolve this issue, do one of the following:
  - Remove the PCIe cards from the system that are not used to free up the MMIO allocation.
  - From the **System Setup** menu, enable the **Memory Mapped I/O above 4GB** option to free up the MMIO allocation.

NOTE: Before working inside your system, follow the safety guidelines listed in the **Safety Instructions** topic in the Installation and Services Manual of your respective server model available on the support site.

Features and fixes in previous releases

Version: 2.17.1

Release Date

November 2022

What's new

- Updated the following:
  - Processor and Memory Reference Code for the second-generation Intel Xeon Processor Scalable Family to IPU 2023.1.
  - The Integrate Intel Purley Refresh Reference Code Version to 626P01.
  - Processor Microcode to version 0x3303 for the second-generation Intel Xeon Processor Scalable Family.
  - Updated SPS to SPS_E5_04.01.04.901.0 (IPU 23.1) for Purley Refresh.

Fixes

- **Issue:** Network boot (PXE/HTTP/HTTPS/iSCSI) in BIOS (legacy) mode always uses Intel NIC E810's port #1 even if other port # is configured.
  Resolution: Recommend users who adopt INTEL E810 NIC network boot (PXE/HTTP/iSCSI) in BIOS boot mode to update the BIOS and latest E810 firmware.

Version: 2.16.1

Release Date

August 2022

What's new

- Updated the following:
  - Processor and Memory Reference Code for the second-generation Intel Xeon Processor Scalable Family to IPU 2022.3.
  - The Integrate Intel Purley Refresh PV Candidate Reference Code Version to 623D09.
  - Integrate AEP Release 1.0.0.3536 files to the Intel Purley Refresh UEFI Source.
  - Firmware updates to address Dell Security Advisory DSA-2022-204.

Fixes

None for this release.

Version: 2.15.1

Release Date

June 2022

What's new

- Updated the following:
  - Processor and Memory Reference Code for the second-generation Intel Xeon Processor Scalable Family to IPU 2022.2.
  - Processor Microcode to version 0x6E05 for the Intel Xeon Processor Scalable Family.
  - The Integrate Intel Purley Refresh PV Candidate Reference Code Version to 622D07.
  - Integrate AEP Release 1.0.0.3534 files to the Intel Purley Refresh UEFI Source.
  - SPS to SPS_E5_04.01.04.804.0 (IPU 22.2) for the Intel Purley Refresh.
- Added support for second source AEP persistent memory (DPN: XVY68, X06-QS) because it is the minimum BIOS version required.

Fixes

- **Issue**: When the Memory Operating Mode option in the Memory Settings menu is set to **MultiRankSpareMode**, multi-bit memory errors are generated in the System Event Log (SEL) or Lifecycle log.
  Resolution: To resolve this issue, upgrade the BIOS version to 2.15.1.
- **Issue**: The Transport Layer Security (TLS) certificate associated with the HTTPS URL is not effectively applied during the HTTPS boot operation. This issue is observed only when using the IPv6 protocol because it breaks the CVE-2021-21571 fix.
  Resolution: To resolve this issue, upgrade the BIOS version to 2.15.1.

Version: 2.14.2

Release Date

April 2022

What's new

- Added enhancements to address the security vulnerabilities (Common Vulnerabilities and Exposures - CVE) such as CVE-2021-0159, CVE-2021-0189, CVE-2021-21131, CVE-2021-33123, CVE-2021-33124, CVE-2021-33159, CVE-2022-21166.
- Updated the "Processor and Memory Reference Code" for the second-generation Intel Xeon Processor Scalable Family to IPU 2022.1.
- Updated the Processor Microcode to version 0x3302 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x6D05 for the Intel Xeon Processor Scalable Family.
- Updated SPS to SPS_E5_04.01.04.700.0 (IPU 2022.1) for Purley Refresh.
- Added Virtual Network File 2 support.
- Enhanced the capability for supporting complex PCIe device.

Fixes

- None for this release.

Version: 2.13.3

Release Date

January 2022

What’s new

- Updated the "Processor and Memory Reference Code" for the second-generation Intel Xeon Processor Scalable Family to IPU 2021.2.
- Updated the Processor Microcode to version 0x320A for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x6C0A for the Intel Xeon Processor Scalable Family.
- Updated SPS to SPS_E5_04.01.04.601.0 (IPU 21.2) for Purley Refresh
- Change memory "Correctable Error Logging" default to Disabled.
- No log for DIMM self-healing status message for Uncorrectable Memory Error.
- Added new BIOS setup option to disable PPR with Uncorrectable Error.
- Updated the S140 Software RAID firmware to version 5.7.0-0006.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures - CVE) such as CVE-2021-28211, CVE-s2021-28210.

Fixes

- Fixed an issue where iDRAC9 UI will allow end-user to define valid IPv6 BIOS Network HTTP URI values with common IPv6 address schemes.
- Fixed an issue where system can perform HTTPS boot to SLES SP3.
- Remove unsupported Software Prefetcher option from setup menu.

Version: 2.12.2

Release Date

July 2021

What’s new

- Support for Microsoft Windows Server 2022 Operating System.
- Updated the S140 Software RAID firmware to version 5.6.0-0002.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures - CVE) such as CVE-2019-14553, CVE-2021-21571.

Fixes

- Fixed system crash with Machine Check Error during MMIO reads when using Intel Optane Persistent Memory 100 Series in Memory Mode.
- Incorrect critical error pop-up message that was seen while exiting iDRAC Settings menu.

Version: 2.11.2

Release Date

April 2021

What’s new

- Updated the "Processor and Memory Reference Code" for the second-generation Intel Xeon Processor Scalable Family to IPU 2021.1.
- Updated the Processor Microcode to version 0x3102 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x6B06 for the Intel Xeon Processor Scalable Family.
- Updated the Purley Refresh PV Candidate Reference Code Version 612D02.
- Updated SPS to SPS_E5_04.01.04.505.0 (IPU 2021.1) for Purley Refresh.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures - CVE) such as CVE-2021-21555, CVE-2021-21556, CVE-2021-21557, CVE-2020-24511, CVE-2020-12358, CVE-2020-12360, CVE-2020-24486.

Fixes

- Fixed BIOS only report partial data in iDRAC/LC for system/setup password after set by SCP from iDRAC.
- Fix Booting to ISO image failed when the iDRAC USB port is Configure as All Ports OFF/AllPortsOff (Dynamic).
- Fix HTTP boot failure with single DNS entry in static IPv4 address mode.

Version: 2.10.2

Release Date

March 2021

What's new

- Updated the Processor Microcode to version 0x3005 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x6A09 for the Intel Xeon Processor Scalable Family.

Fixes

- Fixed an Intel errata reported on IPU 2020.1 and 2020.2 where the system could potentially hang or reboot during POST when "Configuring Memory…" is displayed on the screen. This scenario may be encountered during system boot, where self-heal is attempted. The root cause is a race condition where during the self-heal process, a refresh cycle may not have completed when the CPU issues self-heal related commands to the DRAM.

  The Issue is described in Intel Xeon Processor Scalable Family Specification Update, SKX120 and second-generation Intel Xeon Scalable Processors Specification Update, CLX51.
- Fixed an issue where an invalid location was specified for a self-heal request. This results in self-heal not being performed, which could potentially hang or reboot the system during POST when "Configuring Memory…" is displayed on the screen.

  Note: The Dell PowerEdge BIOS will automatically schedule DIMM self-healing during POST, based on DIMM health monitoring of correctable and uncorrectable errors from previous system boots.

- Updated Intel processor microcode to address the following issues:
  - High Levels of Posted Interrupt Traffic on The PCIe Port May Result in a Machine Check with a TOR Timeout. The Issue is described in the Intel Xeon Processor Scalable Family Specification Update, SKX123 and Second-generation Intel Xeon Scalable Processors Specification Update, CLX52.
  - Some Short Loops of Instructions May Cause a 3-Strike Machine Check without a TOR Timeout. The Issue is described in the Second-generation Intel Xeon Scalable Processors Specification Update, CLX53.

Version: 2.9.3

Release Date

September 2020

What's new

- Updated the "Processor and Memory Reference Code" for the second-generation Intel Xeon Processor Scalable Family to IPU 2020.2.
- Updated the Processor Microcode to version 0x3003 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x6A08 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Intel Management Engine firmware version to 04.01.04.423.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures - CVE) such as CVE-2020-0587, CVE-2020-0588, CVE-2020-0590, CVE-2020-0591, CVE-2020-0592, CVE-2020-0593, CVE-2020-8705, CVE-2020-8738, CVE-2020-8739, CVE-2020-8740, CVE-2020-8755 and CVE-2020-8764.

Fixes

- Updated the "Processor and Memory Reference Code" for the second-generation Intel Xeon Processor Scalable Family to IPU 2020.2.
- Removed the Logical Processor requirement for Monitor/MWait.
- Fixed other miscellaneous issues.

Version: 2.8.2

Release Date

September 2020

What's new

The following are included in 2.8.2 that were released in previous BIOS versions that are no longer available for download.

- Added an option in "DRAM Refresh Delay" in Memory Settings, to disable refresh postponement.
- Updated the "Processor and Memory Reference Code" for the second-generation Intel Xeon Processor Scalable Family to IPU 2020.1.
- The S140 firmware is updated to 5.5.2-0006.
- The memory self-healing feature is added to perform memory self-healing after an uncorrectable error (MEM 0001), burst of correctable errors (MEM 8000), or memory patrol scrub identified uncorrectable error (MEM 9072). Memory self-healing for a MEM 0001, MEM 8000 and MEM 9072 events are initiated after a system restart.
- Updated the Processor Microcode to version 0x2F00 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x69 for the Intel Xeon Processor Scalable Family.
- Updated the Intel Management Engine firmware to version 04.01.04.381.
- Updated the BIOS ACM (authenticated code module) to version 1.7.3.2019.07.12.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures-CVE) such as CVE-2020-0545, CVE-2020-0548, and CVE-2020-0549.

Fixes

Fixed an industry-issue seen on BIOS versions 2.6.3 through 2.8.1 where the system may reset during power-on at the time "Configuring Memory" is displayed on the boot screen. The issue is applicable to DDR4 and NVDIMM-N memory configurations.

The following are included in 2.8.2 that were released in previous BIOS versions that are no longer available for download.

- Issue with the "Monitor/MWait" option in System Profile Settings on 2-socket servers, remaining enabled after selecting disable.
- Issue with "CPU Domain Power Limiting" not capping to target values.
- Issue with MSR 0x1AD which interfered with the new Turbo Ratio Limits has been fixed, without impacting the factory default settings.
- Added the "Balanced Memory Mode" option under "Intel Persistent Memory Performance" in System Profile setting.
- Issue with the memory capacity changing when "Node Interleaving" or "Sub NUMA Cluster" is enabled.
- Fixed an issue with Maximum Payload size because it resulted in a Purple Screen of Death (PSoD) in VMware ESXi when an NVMe drive is hot plugged-in certain configurations.
- Fixed an issue where there was an improper functioning of the MSR 0x1AD (TURBO_RATIO_LIMITS_RATIOS) register.
- Fixed other miscellaneous issues.
- Fixed an issue where the platform may encounter PWR2270 and CPU0000 errors.

Version: 2.5.4

Release Date

February 2020

What’s new

- Updated the "Processor and Memory Reference Code" to 0595.D.04.
- Added the option to enable or disable Correctable Error Logging in the Memory Settings of the System BIOS Settings.
- Enhanced the Lifecycle error messages due to correctable memory errors. You will need to upgrade both the BIOS and iDRAC firmware to make sure that the new messages display correctly in the Lifecycle logs.
- Changed the default setting of Native tRFC Timing for 16 Gb DIMMs to Enabled.
- In some cases, the memory space—indicated by OS as reserved for hardware—is reduced.

Fixes

- Updated a few BIOS Setup help messages.
- Fixed a potential BIOS Recovery failure.
- Issues that were not reported by the Dell customers at the time of current release.

Version: 2.4.8

Release Date

December 2019

What’s new

None for this release.

Fixes

Fixed a continuous reboot issue and Out of Resource error with PCIe IO resource allocation which was observed in the 2.4.7 version.

Version: 2.4.7

Release Date

December 2019

What’s new

- Updated the "Processor and Memory Reference Code to Production Candidate for second-generation Intel Xeon Processor Scalable Family" to PLR2.
- Updated the Processor Microcode to version 0x2C for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x65 for the Intel(R) Xeon Processor Scalable Family.
- Updated the Intel Management Engine firmware to version 04.01.04.354.
- Updated the S140 Software RAID firmware to version 5.5.1-0002.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures-CVE) such as CVE-2019-11090, CVE-2019-11109, CVE-2019-0124, CVE-2019-0151, CVE-2019-0152, CVE-2019-11136, CVE-2019-11137, CVE-2019-11135 and CVE-2019-11139.
- Added the HTTPS certificate management feature.
- Added Setup option to allow 16Gbit density DIMMs to run at native refresh cycle times. This will improve the performance for some DIMMs.

Fixes

- The Turbo Mode feature is effectively enabled.
- Fixed the Max Payload Size in Direct Connect NVMe Configuration for NVMe Hot-plug issue.
- Resolved an issue where a large capacity Initial RAM drive (initrd) could not be successfully allocated.
- Issues that were not reported by the Dell customers at the time of current release.

Version: 2.3.10

Release Date

September 2019

What's new

- Updated the "Processor and Memory Reference Code to Production Candidate for second-generation Intel Xeon Processor Scalable Family" to PLR1.
- Updated the Processor Microcode to version 0x29 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x60 for the Intel(R) Xeon Processor Scalable Family.
- Updated the Intel Management Engine firmware to version 04.01.04.296.
- Enhanced protection for the DIMM Serial Presence Detect (SPD) data.

Fixes

- Upgrading BIOS from 1.6.x (and earlier versions) to 2.2.x can potentially cause BIOS settings to be reset to default values.
- Inconsistencies in the Mellanox CX3 information displayed on the iDRAC GUI in the **Firmware Inventory** section.
- When the boot mode is set to BIOS and you set the date to 1998 in Setup, the Windows Server 2016 date and time displays the year as 2098.
- An Issue Where a Non-Critical Event (MEM9022) may be logged when you select **Cryptographic Erase Disks** from the **Lifecycle Controller** menu.
- Issues that were not reported by the Dell customers at the time of current release.

Version: 2.2.11

Release Date

June 2019

What's new

None for this release.

Fixes

Fixed a rare potential issue which resulted in the server abruptly stopping to respond when a hardware error is reported.

Version: 2.2.9

Release Date

June 2019

What's new

- Added support for the second-generation Intel Xeon Processor Scalable Family.
- Updated the "Processor and Memory Reference Code to Production Candidate for second generation Intel® Xeon® Processor Scalable Family" to MR4.
- Updated the Processor Microcode to version 0x5E for the Intel Xeon Processor Scalable Family.
- Updated the Processor Microcode to version 0x21 for the second-generation Intel Xeon Processor Scalable Family.
- Updated the Intel Trusted Execution Technology (Intel TXT) BIOS Authenticated Code Module (ACM) to version 1.7.1.
- Updated the Intel Management Engine firmware to version 04.01.04.256
- Updated the HPC (High Performance Computing) Workload Profile.
- Added BIOS setting for Intel Adaptive Double DRAM Device Correction (ADDDC) in the **BIOS Settings** menu.
- In the BIOS Settings menu, added BIOS setting for the "Intel SST (Speed Select Technology) Performance Profile" feature.
- Added support for the HTTP Delete Method.
- Added the **Setup** option to allow empty slots to be exposed for PCIe resource allocation. To enable this option, go to **Integrated**

Devices, set the **Empty Slot Unhide** option to **Enabled**. Default is **Disabled** (all empty slots are hidden on the PCIe bus).

- Supports the Boot Sequence placeholder feature for Dell BOSS cards. To enable this feature, under **Boot Settings**, set the **Hard-disk Drive Placeholder** option to **Enabled**. After the next reboot, based on the BOSS card configuration, one or more disk placeholder(s) are displayed in the boot sequence list of the **Boot Settings** page.
- Enhancement to address the security vulnerabilities (Common Vulnerabilities and Exposures—CVE) such as CVE-2018-12126, CVE-2018-12127, and CVE-2018-12130.

Fixes

- Unable to view the log data in the Lifecycle Log files for a few error conditions in the Lifecycle Controller Pre-OS Utility (F10). The following message is displayed — Unable to display Lifecycle Log.
- The TPM PCR1 value is changed after a hardware component is added or removed.
- Machine check that decodes to MC0 (instruction fetch, internal error) with the last bytes of the Status value being F0150. The MCE can also be a combination of MC0 along with MC3 (Internal timer, 3-strike Watchdog), or even MC0, MC3, and MC4 (copy of MC3). Fix is included in the Processor Microcode to version 0x5A for Intel Xeon Processor Scalable Family.
- When the boot mode=BIOS and the USB drive is a part of the HDD list: The ipmitool -I -H -U -P chassis bootdev disk options=persistent IPMI command run to modify the boot sequence also modifies the HDD sequence.
- When booting from an FCOE by using a QLogic 41262 CNA adapter, the BIOS RSoD(Red Screen on Display) may be displayed after applying the server template during boot.
- When changing the BIOS settings by clicking **Configuration→Server Configuration Profile** on the iDRAC GUI, updated the system behavior to complete both the following tasks by running a single job (single SCP file):
  - Change the boot mode from BIOS to UEFI
  - Change the UEFI network settings
- Secure Boot variables were being measured twice (SecureBoot, PK, KEK, db, and dbx) for Trusted Platform Module (TPM) 2.0 version.
- When a BOSS card is installed, a bus fatal error and/or PCIe training error may be reported.
- Power button on the right control panel does not appear to immediately power on a server.
- Microsoft Windows Installer and Windows Boot Loader may fail to start.
- Issues that were not reported by the Dell customers at the time of current release.
- To correctly set the Model-Specific Registers (MSRs) and activate the CPU Turbo Boost feature, the “Number of Turbo Boost Enabled Cores” per processor is fixed in the Setup menu.

Installation instructions

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number** box, type the product name. For example, PowerEdge R830.
3. Select your product from the list that is displayed.
4. Click **Drivers & downloads.**
5. From the **Category** drop-down menu, select **BIOS**.
6. In the **Name** column, expand the hyperlinked BIOS title.
   a. To view information about earlier versions, click **Older versions**.
7. To view information about compatible systems and installation instructions, click **View full driver details**.
8. On the **Driver Details** page, scroll down and expand **Installation instructions**.

   Instructions about downloading and installing Update Packages by using methods such as DRMK, EFI, Linux, and Windows is displayed.
9. Follow the relevant instructions to update the BIOS.

Additional resources and support

Access documents using direct links

You can directly access the documents by using the following links:

URL	Product
www.dell.com/support	The Dell support site

www.dell.com/poweredgemanuals	The Dell PowerEdge server documentation
www.dell.com/idracmanuals	The iDRAC and Lifecycle Controller documentation

Access documents using product search

You can also access documents by searching for your product.

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number...** search box, type the product name. For example, PowerEdge R830.
3. Select your product from the list that is displayed.
4. Click **Manuals & documents**.

License Texts of Components

TianoCore EDK2

SPDX-License-Identifier: BSD-2-Clause-Patent

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice,
   this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,
   this list of conditions and the following disclaimer in the documentation
   and/or other materials provided with the distribution.

Subject to the terms and conditions of this license, each copyright holder
and contributor hereby grants to those receiving rights under this license
a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable
(except for failure to satisfy the conditions of this license) patent
license to make, have made, use, offer to sell, sell, import, and otherwise
transfer this software, where such license applies only to those patent
claims, already acquired or hereafter acquired, licensable by such copyright
holder or contributor that are necessarily infringed by:

(a) their Contribution(s) (the licensed copyrights of copyright holders and
    non-copyrightable additions of contributors, in source or binary form)
    alone; or

(b) combination of their Contribution(s) with the work of authorship to
    which such Contribution(s) was added by such copyright holder or
    contributor, if, at the time the Contribution is added, such addition
    causes such combination to be necessarily infringed. The patent license
    shall not apply to any other combinations which include the
    Contribution.

Except as expressly stated above, no rights or licenses from any copyright
holder or contributor is granted under this license, whether expressly, by
implication, estoppel or otherwise.

DISCLAIMER

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

```
/* ====================================================================
 * Copyright (c) 1998-2023 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
```

* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Brotli

Copyright (c) 2009, 2010, 2013-2016 by the Brotli Authors.

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

Zlib

(C) 1995-2004 Jean-loup Gailly and Mark Adler

  This software is provided 'as-is', without any express or implied
  warranty. In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
     claim that you wrote the original software. If you use this software
     in a product, an acknowledgment in the product documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any source distribution.

  Jean-loup Gailly   Mark Adler
  jloup@gzip.org   madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not*
receiving lengthy legal documents to sign. The sources are provided
for free but without warranty of any kind. The library has been

entirely written by Jean-loup Gailly and Mark Adler; it does not
include third-party code.

If you redistribute modified sources, we would appreciate that you include
in the file ChangeLog history information documenting your changes. Please
read the FAQ for more information on the distribution of modified source
versions.

Oniguruma

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

Libpng

If you modify libpng you may insert additional notices immediately following
this sentence.

libpng versions 1.2.6, August 15, 2004, through 1.2.29, May 8, 2008, are
Copyright (c) 2004, 2006-2008 Glenn Randers-Pehrson, and are
distributed according to the same disclaimer and license as libpng-1.2.5
with the following individual added to the list of Contributing Authors

   Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are
Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are
distributed according to the same disclaimer and license as libpng-1.0.6
with the following individuals added to the list of Contributing Authors

   Simon-Pierre Cadieux
   Eric S. Raymond
   Gilles Vollant

and with the following additions to the disclaimer:

   There is no warranty against interference with your enjoyment of the
   library or against infringement. There is no warranty that our
   efforts or the library will fulfill any of your particular purposes
   or needs. This library is provided with all faults, and the entire
   risk of satisfactory quality, performance, accuracy, and effort is with
   the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are
Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are
distributed according to the same disclaimer and license as libpng-0.96,
with the following individuals added to the list of Contributing Authors:

   Tom Lane
   Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are
Copyright (c) 1996, 1997 Andreas Dilger
Distributed according to the same disclaimer and license as libpng-0.88,
with the following individuals added to the list of Contributing Authors:

John Bowler
Kevin Bracey
Sam Bushell
Magnus Holmgren
Greg Roelofs
Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are
Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors"
is defined as the following set of individuals:

Andreas Dilger
Dave Martindale
Guy Eric Schalnat
Paul Schmidt
Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors
and Group 42, Inc. disclaim all warranties, expressed or implied,
including, without limitation, the warranties of merchantability and of
fitness for any purpose. The Contributing Authors and Group 42, Inc.
assume no liability for direct, indirect, incidental, special, exemplary,
or consequential damages, which may result from the use of the PNG
Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this
source code, or portions hereof, for any purpose, without fee, subject
to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not
be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any
source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without
fee, and encourage the use of this source code as a component to
supporting the PNG file format in commercial products. If you use this
source code in a product, acknowledgment is not required but would be
appreciated.

A "png_get_copyright" function is available, for convenient use in "about"
boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the
files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a
certification mark of the Open Source Initiative.

Glenn Randers-Pehrson
glennrp at users.sourceforge.net
May 8, 2008

Lzma SDK

LZMA SDK is written and placed in the public domain by Igor Pavlov.

Contact Dell

Dell provides several online and telephone-based support and service options. Availability varies by country/region and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues, go to www.dell.com/contactdell.

If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or the product catalog.

2023–02

Rev. A00