Mellanox MLNX-OS® Release Notes for Lenovo SX90Y3452

Software Ver. 3.4.3002

www.mellanox.com

NOTE:
THIS HARDWARE, SOFTWARE OR TEST SUITE PRODUCT ("PRODUCT(S)") AND ITS RELATED DOCUMENTATION ARE PROVIDED BY MELLANOX TECHNOLOGIES "AS-IS" WITH ALL FAULTS OF ANY KIND AND SOLELY FOR THE PURPOSE OF AIDING THE CUSTOMER IN TESTING APPLICATIONS THAT USE THE PRODUCTS IN DESIGNATED SOLUTIONS. THE CUSTOMER'S MANUFACTURING TEST ENVIRONMENT HAS NOT MET THE STANDARDS SET BY MELLANOX TECHNOLOGIES TO FULLY QUALIFY THE PRODUCT(S) AND/OR THE SYSTEM USING IT. THEREFORE, MELLANOX TECHNOLOGIES CANNOT AND DOES NOT GUARANTEE OR WARRANT THAT THE PRODUCTS WILL OPERATE WITH THE HIGHEST QUALITY. ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL MELLANOX BE LIABLE TO CUSTOMER OR ANY THIRD PARTIES FOR ANY DIRECT, INDIRECT, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING, BUT NOT LIMITED TO, PAYMENT FOR 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 FROM THE USE OF THE PRODUCT(S) AND RELATED DOCUMENTATION EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mellanox Technologies
350 Oakmead Parkway Suite 100
Sunnyvale, CA 94085
U.S.A.
www.mellanox.com
Tel: (408) 970-3400
Fax: (408) 970-3403

Mellanox Technologies, Ltd.
Hakidma 26
Ofer Industrial Park
Yokneam 2069200
Israel
www.mellanox.com
Tel: +972 (0)74 723 7200
Fax: +972 (0)4 959 3245

Table of Contents

1 Introduction

This document is the Mellanox MLNX-OS® Release Notes for Lenovo SX90Y3452.

MLNX-OS is a comprehensive management software solution that provides optimal performance for cluster computing, enterprise data centers, and cloud computing over Mellanox SwitchX® family. The fabric management capabilities ensure the highest fabric performance while the chassis management ensures the longest switch up time.

The MLNX-OS documentation package includes the following documents:

- User Manual – provides general information about the scope, organization and command line interface of MLNX-OS as well as basic configuration examples
- Release Notes – provides information on the supported platforms, changes and new features, and reports on software known issues as well as bug fixes

2 Supported Platforms, Firmware, Cables and Licenses

2.1 Supported Switch Systems

Table 1 - Supported Switch Systems

Model Number	Description
SX90Y3452	32-Port 56Gb/s FDR InfiniBand Blade Switch System

2.2 Supported CPU Architecture

- PPC 460

2.3 Supported Firmware

- SwitchX® firmware version 9.3.5080
- SwitchX®-2 firmware version 9.3.5080
- ConnectX®-2 firmware version 2.9.1000 and higher
- ConnectX®-3 firmware version with SwitchX® based systems 2.33.5000 and higher

2.4 Supported Mezzanine

- ConnectX®-2, Mezzanine P/N 90Y3460 (MalayaP), 2.9.1316 and higher
- ConnectX®-2, Mezzanine P/N 90Y3480 (MalayaP-Net), 2.9.1318 and higher
- ConnectX®-3, Mezzanine P/N 90Y3488 (Merlin), 2.32.5100 and higher
- ConnectX®-3, Mezzanine P/N 90Y3484 (Nevada), 2.32.5100 and higher
- ConnectX®-3, Mezzanine P/N 90Y3456 (MalayaX), 2.32.5100 and higher
- ConnectX®-3, Mezzanine P/N 90Y3468 (MalayaX-Net), 2.32.5100 and higher

2.5 Supported CPLD Version

- 1.0.18

2.6 Supported Software Licenses

For the software licenses supported with MLNX-OS® software please refer to the "Licenses" section of the "Getting Started" chapter of the *Mellanox MLNX-OS User Manual*.

2.7 Upgrade From Previous Releases

Older versions of MLNX-OS may require upgrading to one or more intermediate versions prior to upgrading to the latest. Missing an intermediate step may lead to errors. Please refer to Table 2 to identify the correct upgrade order.

Table 2 - Supported Software Upgrades for SX90Y3452

Target Version	Verified Versions From Which to Upgrade
3.4.3002	3.4.2012; 3.4.1120
3.4.2008	3.4.1120; 3.4.0012
3.4.1120	3.4.1110; 3.4.0012; 3.3.5066
3.4.1110	3.4.0012; 3.3.5066
3.4.0012	3.3.5066; 3.3.4402
3.3.5066	3.3.4402; 3.3.4100
3.3.4402	3.3.4100; 3.3.3706
3.3.4100	3.3.3706; 3.2.0596-1
3.3.3706	3.2.0596-1; 3.2.0596
3.2.0596-1	3.2.0596; 3.2.0291
3.2.0596	3.2.0291

For upgrade instructions refer to the section "Upgrading MLNX-OS Software" in *Mellanox MLNX-OS User Manual*.

2.8 Supported Cables

For a list of the Mellanox supported cables please visit the LinkX™ Cables and Transceivers page of the Mellanox Website at http://www.mellanox.com/page/cables?mtag=cable_overview.

When using Mellanox AOC cables longer than 50m use one VL to achieve full wire speed.

3 Changes and New Features

Table 3 - Lenovo SX90Y3452 Changes and New Features

Category	Description
Release 3.4.3002	
User Accounts	Improved logic of AAA authorization map order See the command “aaa authorization map order”
CLI	Improved module status display See command “show module” in the User Manual
XML API	Improved XML interface Refer to MLNX-OS® XML API Reference Guide for more information
Release 3.4.2008	
System Management	Added ONIE support over MLNX-OS platforms
CLI	New user interface for the commands “show guid”, “show lids”, and “show asic version”
CLI	Improved module hierarchy in the output of the commands “show power” and “show temperature”
CLI	Removed CPU component from the output of the command “show inventory”
SNMP	Applied new index scheme for SNMP EntityTable
InfiniBand Switching	New user interface for configuring InfiniBand port speed. See command “interface ib speed <port-speed>” in the InfiniBand chapter.
InfiniBand Switching	New user interface for referencing InfiniBand ports. See “interface ib” commands in the InfiniBand Switching chapter as well as the “Standard MIBs” subsection.
Release 3.4.1120	
General	Removed “sx_” prefix from version numbers in the code
General	Bug fixes
Release 3.4.1110	
WebUI	Added popup Welcome screen when connecting via WebUI See section “Starting the Web User Interface” in the User Manual
Security	Added default passwords to the XML default users See section “User Accounts” in the User Manual
Release 3.4.0012	
Security	Changed the HTTPS default ciphers to TLS.
Configuration Management	Upgraded to VPD version 2.05.
General	Added support for Mellanox OFED 2.3 integration.

Table 3 - Lenovo SX90Y3452 Changes and New Features

Category	Description
Interconnect	Added support for LR4 modules.
SNMP	Added support Mellanox configuration MIB. See section 4.17.1 “SNMP” in the User Manual.
WebUI	Added support for Internet Explorer 11 web browser.
Release 3.3.5066	
General	Bug fix.
Release 3.3.5060	
General	Improved cable info read response time. See the command “show interfaces {ib | eth} transceiver”.
SNMP	Added cable info entries to entPhysicalTable.
SNMP	Added support for SNMP to trigger SNMP test trap via SNMP set command. See section “MLNX-EFM MIB”.
SNMP	Added system identifier (MAC address) to test trap.
Security	Added support for NIST 800-131A.
Release 3.3.4402	
General	The command “show configuration full” is no longer supported.
CLI	Added support for output filtering. See section “Command Output Filtering” in the User Manual.
Release 3.3.4350	
General	Added new certificate hashing algorithm (sha256). See section “Cryptographic (X.509, IPSec)” in the User Manual
Release 3.3.4302	
General	Added End-User License Agreement. See section “Getting Started” in the User Manual.
General	Improved configuration file format.
Power Management	Added support for link width reduction.
Release 3.3.4150	
General	Improved configuration file format.
Release 3.3.4102	
General	Bug fixes.
Release 3.3.4100	
General	Improved debug file upload mechanism. Refer to “file debug-dump” command in the CLI reference guide.

Table 3 - Lenovo SX90Y3452 Changes and New Features

Category	Description
General	Added support for displaying system hardware revision. Refer to “show inventory” command in the CLI reference guide.
SNMP	Added a new extension to entity physical MIB to represent system GUID.
Logging	Added support for event notification to monitor. Refer to Event Notification chapter in the User Manual.
User Interfaces	Improved login timeout mechanism.
Event Notifications	Port up/down event notification to log or terminal. Refer to Event Notification chapter in the User Manual.
Release 3.3.3706	
General	Bug fixes.
Release 3.3.3704	
VPD	Changes to VPD block 1 capability bits.
Release 3.3.3702	
EHCM	Added detailed reasons for failure of CMM upgrade feature.
EHCM	Added fingerprint support for CMM update feature.
EHCM	Image bank 1 represents the active image and image bank 2 represents the non-active image.
VPD	Boot Rom will be reported in image segment 1.
WebUI	Security enhancements.
Release 3.3.3500	
EHCM	Enhancements to software update using CMM feature.
Release 3.3.3400	
EHCM	Added fwImageProtocols OIDs support.
Release 3.3.3000	
General	New Linux kernel 2.6.32.
WebUI	Applied new Apache version. Added temperature critical and warning thresholds to temperature graph.
Software Management	Added support for fetching image from TFTP server using IPv6.
U-boot	Updated u-boot - memory access optimization.
Unbreakable Links	Added Link Level Retry (LLR) support for InfiniBand interfaces.
Modules	Added support for the Mellanox LR4 module, P/N MC2210511-LR4.

Table 3 - Lenovo SX90Y3452 Changes and New Features

Category	Description
Network Interfaces	Added interface range support. By using the interface range configuration mode, a range of ports can be easily configured with the same parameters.
SNMP	SNMP MIB enhancements. General MIBs: Entity-MIB, Entity-Sensor-MIB, Entity-State-MIB and Private MIB restructuring for InfiniBand systems.
Release 3.2.0596	
WebUI	Added support for internal ports in WebUI.
Chassis Management	Added I^2C stability protection.
Configuration Management	Removed “jump-start configuration wizard” feature.
Interfaces	Quality enhancement to link initialization.
System Management	Fixed NTP vulnerability issue.
U-boot	Updated u-boot version.

4 Known Issues

The following sections describe MLNX-OS® known issues in this software release and possible workarounds.

For hardware issues, please refer to the switch support product page.

4.1 General Known Issues

Table 4 - General Known Issues (Sheet 1 of 4)

Index	Category	Description	Workaround
1.	Management Interfaces	The command `reset factory keep-basic` removes management IP configuration.	N/A
2.	Management Interfaces	DHCPv4/v6, VLAN, Zeroconf are not supported on IPoIB.	N/A
3.	Management Interfaces	When re-enabling interface ib0, MTU settings are not saved.	Manually configure MTU settings after re-enabling interface ib0.
4.	Management Interfaces	The CLI command `ip default-gateway <interface>` sets the gateway address to 0.0.0.0 and prevents the user from adding other gateways.	Delete the entry by using the command `no ip default-gateway`.
5.	Management Interfaces	Switch systems may have an expired HTTPS certification.	Generate a new certificate by changing the hostname.
6.	Management Interfaces	Consecutive hostname modification is not supported.	Wait 25 seconds before reattempting to modify the hostname.
7.	NTP	The command `show ntp` always lists the last configured NTP server even if it has been deleted. This output can be safely ignored.	N/A
8.	Software Management	Only one image is allowed to be copied into the system (using the `image fetch` command). The user must remove old image files prior to fetching a new one.	N/A

Table 4 - General Known Issues (Sheet 2 of 4)

Index	Category	Description	Workaround
9.	Software Management	When upgrading to 3.4.1100 and above, before rebooting the system, the following issues may be encountered: • The following error would appear in the log: "[cme.WARNING]: cme_get_swver: Version '3.4.1100' too short!". This error may be safely ignored. • If the agent is down, the command "update -a" from CMM reveals the wrong software version	N/A
10.	User Accounts	If AAA authorization order policy is configured to remote-only, then when upgrading to 3.4.3002 or later from an older MLNX-OS version, this policy is changed to remote-first.	N/A
11.	Configuration Management	After loading a new configuration file, please reboot the system. Otherwise, configuration may not be properly applied and errors may appear in the log.	N/A
12.	Configuration Management	The command set `revert {factory [keep-basic | keep-connect]| saved}` is removed.	Use the equivalent CMM command instead.
13.	Configuration Management	Merging two binary configuration files using the command `configuration merge` is currently not supported.	Use the configuration text file "Apply" option instead.
14.	Configuration Management	When using a large set of configuration files, configuration apply can take more time than usual due to parallel activity of statistics data collecting.	N/A
15.	Configuration Management	Applying a configuration file of one system profile to another is not supported.	N/A
16.	Configuration Management	Sending packets to a non-default port in TFTP transport layer is not supported.	N/A
17.	Logging	"DROPPED MSG" errors may appear during reload (shutdown phase). These errors can be safely ignored.	N/A
18.	Logging	The warning "pgm_set_timeout" may appear in the log. This warning can be safely ignored.	N/A
19.	Logging	During system de-init, the error "[mdreq.ERR]: init(), mdr_main.c:634, build 1: Error code 14014" may appear in the log. This error can be safely ignored.	N/A

Table 4 - General Known Issues (Sheet 3 of 4)

Index	Category	Description	Workaround
20.	Logging	The warning "[mgmtd.WARNING]: Upgrade could not find node to delete: /iss/config/stp/switch/ethernet-default/spanning-tree/mode" may appear in the log. This warning can be safely ignored.	N/A
21.	Logging	When using a regular expression containing | (OR) with the command `show log [not] matching <reg-exp>`, the expression should be surrounded by quotes ("<expression>"), otherwise it is parsed as filter (PIPE) command.	N/A
22.	Logging	Port up/down events on a port quickly toggling states may be displayed in wrong order in the monitoring terminal.	For actual port stats, use the command `show interface`.
23.	User Management	Some RADIUS and TACACS+ configurations keep the user locked out of the machine due to timeout limitation.	Press the reset button for 15 seconds, and then log in using your local authentication. Additionally, fix the configuration to avoid any future timeout issues.
24.	User Management	Logging into the system as USERID from the Serial Connection results in login failure the first attempt.	Log in again. The second attempt will result is successful login.
25.	WebUI	Reversing the time clock can result in WebUI graphs' corrupted data.	Clear the graphs data after setting the clock.
26.	WebUI	Enabling/disabling HTTPS while connected via HTTP to the WebUI may result in temporary loss of connection to the webpage.	Refresh the page or navigate back using the browser's back button.
27.	WebUI	Accessing the WebUI via Firefox with HTTPS is unsupported when working with SSL cipher TLS1.2 level.	Access the WebUI with Firefox only through HTTP.
28.	WebUI	Switching between binary configuration files when connected to the WebUI using HTTPS might result in the following message being displayed: "Switched configuration to '***', which was already the active database." This message is incorrect and can be safely ignored.	N/A
29.	WebUI	If the configured ciphers in versions prior to 3.4.0012 were SSL and TLS ciphers, upgrading to this version will override that. The new default is to allow TLS ciphers only. To enable SSL, please run the command `web https ssl ciphers all`.	N/A

Table 4 - General Known Issues (Sheet 4 of 4)

Index	Category	Description	Workaround
30.	WebUI	When SSH strict mode is activated with TLS 1.2, Firefox does not work properly.	N/A
31.	WebUI	When upgrading to version 3.4.3002, statistics files are reset. As a result, WebUI statistic graphs are reset as well.	N/A
32.	CLI	MLNX-OS support up to 50 CLI session open in parallel.	N/A
33.	CLI	Command output filtering does not support the following commands: • show log • show configuration text files <file>	N/A
34.	SNMP	The error “Cannot find module (MELLANOX-MIB)” may appear in the log when performing rollback to a MLNX-OS version older than 3.3.3000. This error can be safely ignored.	N/A
35.	SNMP	Upon system shutdown, the following error may appear: “[mibd.ERR]: mdc_foreach_binding_ prequeried_parsed(), mdc_main.c”. This error can be safely ignored.	N/A
36.	SNMP	The ifNumbers MIB (OID: 1.3.6.1.2.1.2.1.0) on x86 switch systems displays 42 interfaces while the ifTable displays 40 due to VM management interfaces that are not shown in the ifTable.	N/A
37.	Chassis Management	Upon reaching critical thermal threshold, SR bit 2 is not set although the system is shut down and SR bit 3 is set instead.	N/A

4.2 InfiniBand Known Issues

Table 5 - InfiniBand Known Issues

Index	Category	Description	Possible Workaround
1.	InfiniBand Interfaces	Port hardware speed and width capabilities settings affect port speed and width admin capabilities.	N/A
2.	InfiniBand Interfaces	Setting the port width to 1x in the WebUI and/or CLI is currently not supported.	N/A
3.	InfiniBand Interfaces	Port received packets counter may show random a value when the port is down.	N/A
4.	SNMP	ifPhysAddress OID returns the prefix of the Node GUID of the ib0 management.	N/A

5 Bug Fixes

5.1 General Bug Fixes

The following table describes MLNX-OS® bug fixes in this software release.

Table 6 - General Bug Fixes

Index	Category	Description
1.	SNMP	mellanoxIfVPIIbPortGuid entry is missing for InfiniBand ports.
2.	SNMP	SNMP EntityTable does not refresh immediately after an event.
3.	Chassis Management	The command “show module” displays incorrect “Power” status.
4.	Security	Adding the HTTP header X-Content-Type-Options to all HTTP pages is considered a vulnerability by OWASP ZAP.
5.	User Accounts	Setting AAA authorization mapping to remote-only does not work. Local credentials are still used.
6.	User Accounts	ASCII based authentication using TACACS+ is not functional.
7.	System Management	Received SysRq signals from serial connection (RS232) to USB adapter can cause switch to reboot.
8.	InfiniBand Interface	The no command “no interface ib shutdown” appears in the running config.

5.2 Security Bug Fixes

Table 7 presents the security bug fixes which are added in this MLNX-OS version.

Table 7 - List of Security Bug Fixes

CVE	Description
CVE-2013-7423	The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of request that trigger a call to the getaddrinfo function.
CVE-2014-0475	Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.
CVE-2014-3570	The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.

Table 7 - List of Security Bug Fixes

CVE	Description
CVE-2014-3571	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.
CVE-2014-3572	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.
CVE-2014-7817	The wordexp function in GNU C Library (aka glibc) 2.21 does not enforce the WRDE_NOCMD flag, which allows context-dependent attackers to execute arbitrary commands, as demonstrated by input containing "$((`...`))".
CVE-2014-8176	The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.
CVE-2014-8275	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.
CVE-2014-9297	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided
CVE-2015-0204	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.
CVE-2015-0205	The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.
CVE-2015-0206	Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.

Table 7 - List of Security Bug Fixes

CVE	Description
CVE-2015-0209	Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.
CVE-2015-0285	The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before proceeding with a handshake, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and then conducting a brute-force attack.
CVE-2015-0286	The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.
CVE-2015-0287	The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.
CVE-2015-0288	The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.
CVE-2015-0289	The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.
CVE-2015-0292	Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.
CVE-2015-0293	The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.
CVE-2015-1789	The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

Table 7 - List of Security Bug Fixes

CVE	Description
CVE-2015-1790	The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.
CVE-2015-1791	Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.
CVE-2015-1792	The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.
CVE-2015-1798	The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p2 requires a correct MAC only if the MAC field has a nonzero length, which makes it easier for man-in-the-middle attackers to spoof packets by omitting the MAC.
CVE-2015-1799	The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 3.x and 4.x before 4.2.8p2 performs state-variable updates upon receiving certain invalid packets, which makes it easier for man-in-the-middle attackers to cause a denial of service (synchronization loss) by spoofing the source IP address of a peer.
CVE-2015-3456	The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a denial of service (out-of-bounds write and guest crash) or possibly execute arbitrary code via the (1) FD_CMD_READ_ID, (2) FD_CMD_DRIVE_SPECIFICATION_COMMAND, or other unspecified commands, aka VENOM. Though the VENOM vulnerability is also agnostic of the guest operating system, an attacker (or an attacker's malware) would need to have administrative or root privileges in the guest operating system in order to exploit VENOM.
CVE-2015-4000	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.
CVE-2015-5119	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

6 Submitting a Service Request

The Mellanox® Support Center is at your service for any issues. You may access the Warranty Service through the Web Request Form by using the following link:

http://www.mellanox.com/content/pages.php?pg=support_index.