Extreme®
Connect Beyond the Network

145 Rio Robles
San Jose, CA 95134
+1 877-801-7082

Customer Release Notes

Extreme Networks Intrusion Prevention System

Software Version 8.3 Maintenance Release 2 (Build 350)

March 4, 2016

INTRODUCTION:

This maintenance release contains patches to mitigate several software vulnerabilities, and includes a fix for one defect in the EMS component. There are no updates to the host sensor or network sensor in this release. The Extreme Networks Intrusion Prevention System was previously referred to as Dragon Intrusion Defense System.

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

To view the latest version of the *Customer Release Notes*, go to the Extreme Networks Support Portal, IPS page: https://extranet.extremenetworks.com/downloads/pages/IPS.aspx. The v8.3 release notes are posted in the **Documentation** tab.

RECENT PRODUCT SOFTWARE RELEASE HISTORY:

Status	Version No.	Type	Release Date
Current Version	8.3 Build 350	Maintenance Release	1/15/16
Previous Version	8.3 Build 347	Maintenance Release	3/11/15
Previous Version	8.3	Feature Release	7/18/14
Previous Version	8.2	Feature Release	11/22/13
Previous Version	8.1	Feature Release	5/8/13
Previous Version	8.0	Feature Release	11/02/12

INSTALLATION / UPGRADE INFORMATION:

IMPORTANT NOTES ABOUT UPGRADING TO v8.3 MR2

- If upgrading the EMS without upgrading the O/S to the latest appliance image, you must ensure that the OpenSSL library on this system is version 1.0.1 or higher (see Minimum Required Third-Party Software Versions on page 6 for more information).
- The O/S of a network sensor running version 8.3 or 8.1 MR1 can be upgraded to 8.3 MR2 if the system has Internet access. If the system does not have Internet access, you must perform a clean install of the 8.3 MR2 ISO from a flash drive or DVD. This will wipe the disk, so you should make a note of the network settings as well as the event channel and config channel settings before you start the installation.
- The O/S of an EMS running version 8.3 or 8.3 MR1 can be upgraded “in place” to 8.3 MR2 if and only if the EMS server has Internet access. If the EMS does not have a working connection to the Internet, you will not be able to perform an “in place” upgrade. If an in place upgrade of the EMS cannot be performed, you must

back-up your policy and event data and do a clean install of the 8.3 MR2 ISO, and then restore your backed-up data. It is recommended that you call GTAC for assistance.

- You cannot upgrade an EMS of an pre-8.3 version directly to 8.3 MR2; you must first upgrade to 8.3.
- To perform an in place O/S upgrade of an 8.3 EMS or network sensor, follow these instructions:

1. Download the script file, DAR6.0-8.3_64bit_350_14_Upgrade.bin, from the Extreme Networks Support Portal: https://extranet.extremenetworks.com/downloads/pages/IPS.aspx

Note:

To run the upgrade script, you must be logged in to the EMS appliance as root.

2. Copy the DAR6.0-8.3_64bit_350_14_Upgrade.bin file to the /opt directory of the EMS appliance to be upgraded.
3. In the /opt directory, run the DAR6.0-8.3_64bit_350_14_Upgrade.bin script.

```
# ./DAR6.0-8.3_64bit_350_14_Upgrade.bin
```

The upgrade process indicates when it has finished upgrading and updating your files.

```
# root@dragon2:~# ./DAR6.0-8.3_64bit_350_14_Upgrade.bin
Verifying archive integrity... All good.
Uncompressing
update..........................................................................
................................................................................
.................

This is the Extreme Dragon ISO update script. This requires internet access in
order to complete.

Current OS version is 10.04
Checking internet connectivity..
Performing upgrade, this could take a while..
OS Upgrade was successful. Applying updates..
Installing updated packages..
Removing udev net generator rules
Updating drivers..
Upgrade completed.

Please reboot to complete the upgrade.
```

4. Reboot the appliance. The OS updates could take several minutes to complete after the reboot.

Note:

The script file only upgrades the platform operating system. You must still upgrade the EMS by downloading and installing the `EmsServer_Linux_64bit_8.3.0_350.tar.gz` file from the Extreme Networks Support Portal.

Note:

IPS v8.3 MR2 (build 350) contains no changes to the host sensors or network sensor. IPS v8.3 (build 333) host sensors and network sensors are fully compatible with an EMS upgraded to IPS v8.3 MR2 (build 350).

KNOWN ISSUES IN RELEASE 8.3 MR2:

Issues Addressed	I.D.
[11001] A defect in the EMS that could cause log files to grow to huge sizes and consume all available disk space has been corrected.	01173098

Vulnerabilities Mitigated	I.D.
[10985] VULN: krb5 USN-2498-1 CVE-2014-5351, CVE-2014-5352, CVE-2014-5353 CVSS=9.0	N/A
[10991] Bar Mitzvah weak ciphers in SSL and TLS protocol	N/A
[10993] CVE-2015-1798 and CVE-2015-1799	N/A
[10996] CVE-2015-5366	1135631
[10998] CVE-2008-5161	1162291

KNOWN RESTRICTIONS AND LIMITATIONS IN RELEASE 8.3 MR2:

Installation
[11026] When running the installation from the command line, the following benign error message is displayed: `strings: '/lib/libc.so.6': No such file`
[11009] After upgrading the OS, it is normal to see several “Template parse error” messages and also some “Unhandled error from nih_dbus_error_raise” messages in the dist_upgrade.log file.

Network Sensor
[10035] Enabling performance reporting on a networks sensor using a DNIC-HS2X10G-S interface will cause the sensor to crash.

To report an issue not listed in this document, contact our Global Technical Support staff.

KNOWN ISSUES ADDRESSED IN PREVIOUS RELEASES:

For information about known issues addressed in previous releases, see the v8.3, v8.2, v8.1, and v8.0 *Customer Release Notes*.

APPLIANCE INSTALLATION DOCUMENTATION

Extreme Networks IPS Current Generation Appliances

The Extreme Networks IPS v8.3 installation documentation includes an *Appliance Hardware Installation Guide* for current generation appliances (rev 5x, 6a, and above).

SYSTEM REQUIREMENTS:

Supported Platforms

Network Sensor

The IPS Network Sensor is supported only on Extreme Networks IPS appliances.

The IDS Network Sensor is supported on Extreme Networks IPS appliances and also can be installed on the following platforms, whether installed as a host OS or as a guest OS on VMware ESX Server version 5.x:

Operating System	Architecture	Version
Red Hat Enterprise Linux	IA-32, 64	5, 6
CentOS	IA-32, 64	5, 6

Host Sensor

Extreme Networks IPS Host Sensor is now supported when installed on any supported OS that is itself running on a virtual machine of a VMware ESX Server (version 4.x or 5.x) host. Host Sensor is also supported on AIX 5.3 and 6.1 running in logical partitions (LPARS), and on Solaris 10 running in logical domains (LDOMS) on supported platforms.

The Host Sensor can be installed on the following platforms:

Operating System	Architecture	Version
AIX	Power PC 32	5.2, 5.3, 6.1
AIX	Power PC 64	5.2, 5.3, 6.1
SUSE	IA-32, 64	9, 10
CentOS	IA-32, 64	5, 6
HP-UX	PA-RISC 32	11
HP-UX	PA-RISC 64	11 with patch PHSS_33033 applied
Red Hat Enterprise Linux	IA-32, 64	5, 6
Solaris	Sparc	9, 10 with latest jumbo patch applied
Solaris	Sparc 64-bit	10
Windows	IA-32, X86-64	2003 Server
Windows	IA-32, X86-64	2008 Server
Windows	IA-32, X86-64	Windows 7
Windows	X86-64	2008 Server R2
Windows	X86-64	2012 Server
Extreme Networks IPS ISO	All Extreme Networks IPS appliances	Ubuntu with 3.3.x kernel

EMS/Reporting Server and Integrated Sensor/Server

The Extreme Networks IPS EMS Server is supported on Extreme Networks IPS appliances. The EMS Server is also supported when installed on any supported OS that is itself running on a virtual machine of a VMware ESX Server 4.x or 5.x host.

You can also install the EMS on the following platforms:

Operating System	Architecture	Version
Red Hat Enterprise Linux	IA-32, 64	5, 6
CentOS	IA-32, 64	5, 6

Minimum Hardware Requirements

The minimum hardware requirements have been updated with this release. Please ensure that your hardware supports these minimum requirements prior to installation or upgrade.

Network Sensor

Intel (Linux):

- 2.66 GHz Xeon 3070 Processor
- 20 GB Disk Space
- 2 GB RAM
- Intel-based network interface card

EMS / Reporting Server and Integrated Sensor/Server:

Intel (Linux):

- 2.66 GHz Xeon 3070 Processor
- 60 GB Disk Space – dependent on data retention requirements
- 4 GB RAM
- Intel-based network interface card

Virtual Sensor Memory Requirements

- 1 GB RAM for one virtual sensor
- Add 512 MB for each additional virtual sensor, up to a maximum of 32 virtual sensors.

Software Requirements

Minimum Required Third-Party Software Versions

NOTE:

This section does not apply to Extreme Networks IPS Appliances, which come with all required software pre-installed.

The following third-party software products are required to be installed on machines running the EMS/Reporting Server or the Integrated Sensor/Server:

gzip/gunzip	1.2.4
Perl	5.12 or higher
Perl-dbd-mysql	4.014 or higher
Perl-dbi	1.609 or higher
OpenSSL	1.0.1 or higher
Sendmail	8.12.10 (Alarmtool MTA)

IPS GUI Requirements

The IPS GUI is supported by the following Web browsers:

- Chrome 47
- Firefox 43
- Internet Explorer 11

The IPS GUI requires 2 GB RAM (4 GB RAM recommended).

GLOBAL SUPPORT:

By Phone:	+1 877-801-7082 (toll-free in U.S. and Canada)
	For the toll-free support number in your country: www.extremenetworks.com/support/
By Email:	support@extremenetworks.com
By Web:	www.extremenetworks.com/support/
By Mail:	Extreme Networks, Inc. 145 Rio Robles San Jose, CA 95134

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.