Extreme Networks Security Analytics Release Notes

For Software Version 7.7.2.8

9035041-08

Published January 2018

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Table of Contents

Preface

Related Publications

The ExtremeSecurity product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

ExtremeSecurity Analytics & SIEM

- *ExtremeSecurity API Reference Guide*
- *ExtremeSecurity Application Configuration Guide*
- *ExtremeSecurity Ariel Query Language Guide*
- *ExtremeSecurity DSM Configuration Guide*
- *ExtremeSecurity Hardware Guide*
- *ExtremeSecurity Installation Guide*
- *ExtremeSecurity Juniper NSM Plug-in User Guide*
- *ExtremeSecurity Log Manager Administration Guide*
- *ExtremeSecurity Log Manager Users Guide*
- *ExtremeSecurity Managing Log Sources Guide*
- *ExtremeSecurity Offboard Storage Guide*
- *ExtremeSecurity Release Notes*
- *ExtremeSecurity Risk Manager Adapter Configuration Guide*
- *ExtremeSecurity Risk Manager Getting Started Guide*
- *ExtremeSecurity Risk Manager Installation Guide*
- *ExtremeSecurity Troubleshooting System Notifications Guide*
- *ExtremeSecurity Upgrade Guide*
- *ExtremeSecurity Vulnerability Assessment Configuration Guide*
- *ExtremeSecurity Vulnerability Manager User Guide*
- *ExtremeSecurity WinCollect User Guide*
- *Extreme SIEM Administration Guide*
- *Extreme SIEM Getting Started Guide*
- *Extreme SIEM High Availability Guide*
- *Extreme SIEM Tuning Guide*
- *Extreme SIEM User Guide*
- *Migrating ExtremeSecurity Log Manager to Extreme SIEM*

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.

- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- Extreme Portal — Search the GTAC knowledgebase, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- The Hub — A forum for Extreme customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

1 About the ExtremeSecurity V7.7.2.8 Release Notes

Patch Installation Instructions
V7.7.2.8 Firmware Releases

These release notes cover ExtremeSecurity for release V7.7.2.8, including patches. These notes cover:

- Firmware support
- Fixes
- Known Issues

For the patch upgrade procedure, see Patch Installation Instructions.

Patch Installation Instructions

Before you begin, ensure that you take the following precautions:

- To avoid access errors in your log file, close all open ExtremeSecurity sessions.
- The fix pack for ExtremeSecurity cannot be installed on a managed host that is at a different software version from the Console. All appliances in the deployment must be at the same software revision to patch the entire deployment.
- Verify that all changes are deployed on your appliances. The patch cannot install on appliances that have changes that are not deployed.
- The .SFS file is only capable of upgrading existing ExtremeSecurity installations. A V7.7.2.8 ISO is available for administrators to want to install a new appliance or virtual machine. Administrators who want to do a new install need to review the *ExtremeSecurity Installation Guide*.

Fix packs are installed by using an SFS file. The fix pack can update any appliance attached to the ExtremeSecurity Console that is at the same software version as the Console.

The instructions guide administrators through the process of upgrading an existing ExtremeSecurity at V7.7.2.4 (7.2.4.983526) or later to the latest software version. If the administrator is interested in updating appliances in parallel, see: QRadar: How to Update Appliances in Parallel.

Remember
If you already installed ExtremeSecurity V7.7.2.8 Patch 8 Interim Fix 01, there is no need to install this update as there are no new resolved issues. This release follows up V7.7.2.8 Patch 8 Interim Fix 01 for customers who are not yet on V7.7.2.8 Patch 8 to prevent them from installing both Patch 8 and an interim fix.

1 Download the fix pack to install ExtremeSecurity V7.7.2.8 Patch 11 from the **Software** tab of the Extreme SIEM downloads page (https://extranet.extremenetworks.com/downloads/Pages/SIEM.aspx).

2 Using SSH, log in to your system as `root`.

3 Copy the patch file to the `/tmp` directory on the SIEM Console.

Note
If space in `/tmp` is limited, copy the patch file to another location with sufficient space.

4 Create the `/media/updates` directory:

```
mkdir –p /media/updates
```

5 Change to the directory where you copied the patch file: `cd <directory>`

For example: `cd /tmp`

6 Mount the patch file to the /media/updates directory:

```
mount -o loop -t squashfs 728_QRadar_patchupdate-7.2.8.<build-
number>.sfs /media/updates
```

7 Run the patch installer:

```
/media/updates/installer
```

Note
The first time you use the patch installer script, expect a delay before the first patch installer menu is displayed.

8 Using the patch installer, select **all**.

- The **all** option updates the software on all appliances in the following order:

1 Console

Note
No order required for remaining appliances except console. All remaining appliances can be updated in any order the administrator requires.

- If you do not select the **all** option, you must select your Console appliance.

As of ExtremeSecurity V7.7.2.6 Patch 4 and later, administrators are only provided the option to update **all** or update the Console appliance as the managed hosts are not displayed in the installation menu. After the Console is patched, a list of managed hosts that can be updated is displayed in the installation menu. This change was made starting with ExtremeSecurity V7.7.2.6 Patch 4 to ensure that the Console appliance is always updated before managed hosts to prevent upgrade issues.

If administrators want to patch systems in series, they can update the Console first, then copy the patch to all other appliances and run the patch installer individually on each managed host. The Console must be patched before you can run the installer on managed hosts.

If your Secure Shell (SSH) session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the patch installation resumes.

A summary of the fix pack installation advises you of any managed host that were not updated.

Tip
If the fix pack fails to update a managed host, you can copy the fix pack to the host and run the installation locally. After all hosts are updated, administrators can send an email to their team to inform them that they will need to clear their browser cache before logging in to the SIEM interface.

9 After the patch completes and you have exited the installer, type the following command:

```
umount /media/updates
```

10 After all hosts are updated, administrators can send an email to their team to inform them that they will need to clear their browser cache before logging in to the SIEM interface.

A summary of the fix pack installation advises you of any managed host that were not updated. If the fix pack fails to update a managed host, you can copy the fix pack to the host and run the installation locally.

After all hosts are updated, administrators can send an email to their team to inform them that they will need to clear their browser cache before logging in to the Extreme SIEM interface.

V7.7.2.8 Firmware Releases

Status	Firmware Version	Product Type	Release Date
Current Version	V7.7.2.8 Build 20171213225424	Customer Software	January 29, 2018
Previous Version	V7.7.2.8 Build 20171013131303	Customer Software	January 04, 2018
Previous Version	V7.7.2.8Build 20170726184122	Customer Software	September 14, 2017
Previous Version	V7.7.2.8Build 20170530170730	Customer Software	August 16, 2017
Previous Version	V7.7.2.8Build 20170403173410	Customer Software	April 21, 2017
Previous Version	V7.7.2.8Build 20170224202650	Customer Software	March 16, 2017
PreviousVersion	V7.7.2.8Build 20170105231716	Customer Software	January 23, 2017
Previous Version	V7.7.2.8 Build 20161118202122	Customer Software	December 6, 2016
Previous Version	V7.7.2.8 Build 20160920132350	Customer Software	November 8, 2016

2 Release Notes for ExtremeSecurity V7.7.2.8 Patch 11

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 11.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

ExtremeSecurity V7.7.2.8 Patch 11 is released and resolves field issues reported from users and administrators. An additional security bulletin was added to this release note on December 4th, 2017.

Before installing this update, there are several important changes that administrators should be aware of if they did not install a previous ExtremeSecurity release (V7.7.2.8 Patch 7, Patch 8, or Patch 9). This message was included in the V7.7.2.8 Patch 10 release notes for visibility:

- TLSv1 is disabled in ExtremeSecurity V7.7.2.8 Patch 7 and later. This change was originally completed in ExtremeSecurity V7.7.3.0 and has been ported to the ExtremeSecurity V7.7.2.8 software stream as of V7.7.2.8 Patch 7. This means that Tomcat will no longer listen and actively refuse browser connections using TLSv1.0 after updating to ExtremeSecurity V7.7.2.8 Patch 10. Browsers will be required to use TLSv1.1 or TLSv1.2 to authenticate to ExtremeSecurity SIEM. This should only impact users with older or legacy browsers.
- The installation of ExtremeSecurity V7.7.2.8 Patch 10 and later updates the Java version to Java 8. This change was released as part of V7.7.2.8 Patch 7, but is also being noted for administrators in the release notes for V7.7.2.8 Patch 10 to ensure this change is communicated.
- The Master Console v0.10.0 or v0.11.0 is not supported on ExtremeSecurity V7.7.2.8 Patch 7 or later, including V7.7.2.8 Patch 10 due to changes made with Java 8 and TLSv1.0 connections as described above. Administrators who require the Master Console should not upgrade to a version above ExtremeSecurity V7.7.2.8 Patch 6.
- Administrators with managed WinCollect agents at version V7.7.2.3 or earlier can be impacted by disabled ciphers in ExtremeSecurity V7.7.2.8 Patch 7 and later. It is recommended that administrators with managed WinCollect agents upgrade to the latest WinCollect agent version. Administrators who have upgraded to WinCollect V7.7.2.4 or later are not impacted by this issue and administrators with Stand-alone WinCollect agents are also not impacted.

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRSIEM-20171213225424 to upgrade to ExtremeSecurity V7.7.2.8 Patch 11:

Current ExtremeSecurity Version	Upgrades to ExtremeSecurity V7.7.2.8 Patch 10?
ExtremeSecurity V7.7.2.3 (any patch level) or earlier	No, a minimum of ExtremeSecurity V7.7.2.4 is required.
ExtremeSecurity V7.7.2.4 (any patch level)	Yes

Current ExtremeSecurity Version	Upgrades to ExtremeSecurity V7.7.2.8 Patch 10?
ExtremeSecurity V7.7.2.5 (any patch level)	Yes
ExtremeSecurity V7.7.2.6 (any patch level)	Yes
ExtremeSecurity V7.7.2.7 (any patch level)	Yes
ExtremeSecurity V7.7.2.8 (any patch level)	Yes

The 7.2.8-QRADAR-QRSIEM-20171213225424 fix pack can upgrade ExtremeSecurity V7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for QRadar. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than ExtremeSecurity V7.7.2.4, you must upgrade to ExtremeSecurity V7.7.2.4 before proceeding to ExtremeSecurity V7.7.2.8.

Important
A ExtremeSecurity V7.7.2.8 ISO is available on IBM Fix Central for administrators to want to install a new appliance or virtual machine. Administrators who want to complete a new install need to review the *ExtremeSecurity Installation Guide*.

Resolved Issues

Note
Legend: ** characters are displayed next to an APAR indicate that this issue was discovered in another software version, such as ExtremeSecurity V7.7.3.0 and a fix was created to resolve this issue in V7.7.2.8 Patch 10. Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 1: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 11

Product	Component	Number	Description
EXTREMESECURITY	LOG SOURCES	IV99511**	LOG SOURCE GROUP WINDOW CAN SOMETIMES FAIL TO LOAD WHEN GREATER THAN 1000 LOG SOURCES EXIST IN A GROUP
QRADAR VULNERABILITY MANAGER	SCAN POLICY	IV98930	'FAILED TO LOAD DATA' MESSAGE WHEN TRYING TO ADD NEW VULNERABILITIES INTO A PATCH SCAN POLICY
EXTREMESECURITY	DASHBOARDS	IV98873**	THE MESSAGE 'THERE WAS AN ERROR DOWNLOADING THIS ITEM' CAN SOMETIMES BE DISPLAYED IN A DASHBOARD WIDGET
EXTREMESECURITY	APPLICATIONS	IV98744	HOSTCONTEXT OUT OF MEMORY INSTANCES CAN SOMETIMES OCCUR DURING BACKUP OF EXTREMESECURITY APPS
EXTREMESECURITY	LOG SOURCES	IV98493	BULK ADD/EDIT OF MORE THAN 100 LOG SOURCES CAN FAIL
EXTREMESECURITY	LOG SOURCES	IV98436	UNABLE TO PERFORM A BULK ADD OF LOG SOURCES

Table 1: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 11 (continued)

EXTREMESECURITY	API	IV98260	COMMA'S ARE TREATED AS "OR" IN QUICK FILTER SEARCHES CAUSING VARIED SEARCH RESULTS
EXTREMESECURITY	SEARCHES	IV98190	'FAILED TO LOAD DATA' MESSAGE WHEN TRYING TO ADD NEW VULNERABILITIES INTO A PATCH SCAN POLICY
EXTREMESECURITY	SEARCHES	IV98100	ADDING A REGEX FILTER TO A SEARCH CAN GENERATE ERROR 'FATAL EXCEPTION IN VALIDATIONEXCEPTION: THIS IS NOT A VALID...'
EXTREMESECURITY	LOG SOURCE EXTENSIONS	IV97847	LOG SOURCE EXTENSIONS CAN EXPERIENCE SINGLE-DIGIT DATE PARSING ISSUES
EXTREMESECURITY VULNERABILITY MANAGER	VULNERABILITY ASSIGNMENT	IV97523	UNABLE TO ADD NEW CIDR RANGES IN VULNERABILITY ASSIGNMENT SCREEN
EXTREMESECURITY	SEARCHES	IV97151**	'THE SERVER ENCOUNTERED AN ERROR READING ONE OR MORE FILES' WHEN PERFORMING A LOG ACTIVITY SEARCH
EXTREMESECURITY	DOCKER	IV95751**	'THE SERVER ENCOUNTERED AN ERROR READING ONE OR MORE FILES' WHEN PERFORMING A LOG ACTIVITY SEARCH
EXTREMESECURITY	REPORTS	IV95248**	'THE SERVER ENCOUNTERED AN ERROR READING ONE OR MORE FILES' WHEN PERFORMING A LOG ACTIVITY SEARCH
EXTREMESECURITY	PATCH	IV93699	PATCH TO 7.2 MR1 HANGS ON REBOOT IF A NEW SESSION IS OPENED PRIOR TO REBOOTING
EXTREMESECURITY	OFFENSES	IV91301**	'OFFENSE SEARCH EXCLUSION FILTERS CONTAINING A DEFINED NETWORK HIERARCHY PARAMETER DO NOT RESPECT THE EXCLUSION
EXTREMESECURITY	CUSTOM RULES ENGINE	IV85841	EXTREMESECURITY SYSTEM DEGRADATION AND/OR DROPPED EVENTS CAN CAUSED BY SOME VULNERABILITY CRE TESTS
EXTREMESECURITY RISK MANAGER	GRAPHS	IV87193	THE QRM 'DOWNLOAD IMAGE' BUTTON GENERATES ERROR 'THE GRAPH WAS TOO LARGE TO DOWNLOAD.' INCORRECTLY
EXTREMESECURITY	DEPLOYMENT ACTIONS	IV78428	ADDING OR RE-ADDING A EXTREMESECURITY MANAGED HOST CAN SOMETIMES FAIL
EXTREMESECURITY VULNERABILITY MANAGER	VULNERABILITIES	IJ02090**	NEWLY CONFIGURED VULNERABILITY EXCEPTIONS CAN SOMETIMES BE DUPLICATED
EXTREMESECURITY	USER ROLES	IJ01112	NON ADMIN USERS WITH LIMITED USER ROLES MAY NOT BE ABLE TO FILTER BY CATAGTORIES
EXTREMESECURITY	CUSTOM EVENT PROPERTIES	IJ00489	COMMAS ARE SWITCHED TO 'OR' WHEN MULTIPLE CUSTOM EVENT PROPERTIES ARE CONTAINED IN A SEARCH
EXTREMESECURITY	USER INTERFACE	IJ00416	LOG AND NETWORK ACTIVITY EXPORTS TO CSV DISPLAY INCORRECT COLUMN NAMES

Table 1: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 11 (continued)

EXTREMESECURITY	AQL	IJ00327	AQL SEARCH WITH 'REFERENCESETCONTAINS' CAN FILL QRADAR LOGS WITH "THE USERSESSION OBJECT IN SESSIONCONTEXT IS NULL...
EXTREMESECURITY	DATA NODES	IJ00141**	DISK MAINTENANCE DELETES /STORE/ARIEL/ FLOWS (RECORDS AND PAYLOADS) DIRECTORY ON DATANODES THAT RECEIVE EVENTS ONLY
EXTREMESECURITY	REPORTS	IJ00069**	'ERROR GENERATING SQL CHART' WHEN RUNNING A REPORT WITH "TIME" SET AS THE HORIZONTAL X-AXIS
EXTREMESECURITY	AQL	IJ00066	TABLE REPORTS USING ACCUMULATED AQL DATA DISPLAY INCORRECT COLUMNS
EXTREMESECURITY VULNERABILITY MANAGER	SCANNERS	IJ00034	VULNERABILITY DMZ EXTERNAL SCAN USING AUTHENTICATED PROXY OPTIONS DOES NOT WORK AS EXPECTED

3 Release Notes for ExtremeSecurity V7.7.2.8 Patch 10

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 10.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

ExtremeSecurity V7.7.2.8 Patch 10 is released and resolves 46 field issues reported from users and administrators. An additional security bulletin was added to this release note on December 4th, 2017.

Before installing this update, there are three important changes that administrators should be aware of if they did not install the previous ExtremeSecurity release (V7.7.2.8 Patch 7, Patch 8, or Patch 9). This message is being included in the V7.7.2.8 Patch 10 release notes for visibility:

- TLSv1 is disabled in ExtremeSecurity V7.7.2.8 Patch 7 and later. This change was originally completed in ExtremeSecurity V7.7.3.0 and has been ported to the ExtremeSecurity V7.7.2.8 software stream as of V7.7.2.8 Patch 7. This means that Tomcat will no longer listen and actively refuse browser connections using TLSv1.0 after updating to ExtremeSecurity V7.7.2.8 Patch 10. Browsers will be required to use TLSv1.1 or TLSv1.2 to authenticate to ExtremeSecurity SIEM. This should only impact users with older or legacy browsers.
- The installation of ExtremeSecurity V7.7.2.8 Patch 10 and later updates the Java version to Java 8. This change was released as part of V7.7.2.8 Patch 7, but is also being noted for administrators in the release notes for V7.7.2.8 Patch 10 to ensure this change is communicated.
- The Master Console v0.10.0 or v0.11.0 is not supported on ExtremeSecurity V7.7.2.8 Patch 7 or later, including V7.7.2.8 Patch 10 due to changes made with Java 8 and TLSv1.0 connections as described above. Administrators who require the Master Console should not upgrade to a version above ExtremeSecurity V7.7.2.8 Patch 6.
- Administrators with managed WinCollect agents at version V7.7.2.3 or earlier can be impacted by disabled ciphers in ExtremeSecurity V7.7.2.8 Patch 7 and later. It is recommended that administrators with managed WinCollect agents upgrade to the latest WinCollect agent version. Administrators who have upgraded to WinCollect V7.7.2.4 or later are not impacted by this issue and administrators with Stand-alone WinCollect agents are also not impacted.

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRSIEM-20171013131303 to upgrade to ExtremeSecurity V7.7.2.8 Patch 10:

Current ExtremeSecurity Version	Upgrades to ExtremeSecurity V7.7.2.8 Patch 9?
ExtremeSecurity V7.7.2.3 (any patch level) or earlier	No, a minimum of ExtremeSecurity V7.7.2.4 is required.
ExtremeSecurity V7.7.2.4 (any patch level)	Yes
ExtremeSecurity V7.7.2.5 (any patch level)	Yes
ExtremeSecurity V7.7.2.6 (any patch level)	Yes
ExtremeSecurity V7.7.2.7 (any patch level)	Yes
ExtremeSecurity V7.7.2.8 (any patch level)	Yes

The 7.2.8-QRADAR-QRSIEM-20171013131303 fix pack can upgrade ExtremeSecurity V7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for QRadar. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than ExtremeSecurity V7.7.2.4, you must upgrade to ExtremeSecurity V7.7.2.4 before proceeding to ExtremeSecurity V7.7.2.8.

Important

A ExtremeSecurity V7.7.2.8 ISO is available on IBM Fix Central for administrators to want to install a new appliance or virtual machine. Administrators who want to complete a new install need to review the *ExtremeSecurity Installation Guide*.

Known Issue

There is a known issue in ExtremeSecurity V7.7.2.8 Patch 10 that can impact Internet Explorer 11 and Edge browsers. It has been reported that Internet Explorer 11 might not display an event details pop-up window when a multiple(x) value is selected in a sub-search. This issue only impacts IE11 and Edge broswers. An APAR has been opened for this issue and an investigation is ongoing.

Table 2: Known issue in ExtremeSecurity V7.7.2.8 Patch 10

Product	Component	Number	Description
EXTREMESECURITY	USER INTERFACE	IJ00800	"HTTP ERROR 400" ERROR WHEN DRILLING DOWN INTO SEARCH RESULTS USING INTERNET EXPLORER 11 AND EDGE WEB BROWSER

Resolved Issues

Note

Legend: ** characters are displayed next to an APAR indicate that this issue was discovered in another software version, such as ExtremeSecurity V7.7.3.0 and a fix was created to resolve this issue in V7.7.2.8 Patch 10. Some APAR links in the table below might take 24 hours to display properly after a software release.

Table 3: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 10

Product	Component	Number	Description
EXTREMESECURITY	SECURITY BULLETIN	CVE-2015-6420	APACHE COMMONS COLLECTION AS USED IN IBM EXTREMESECURITY SIEM IS VULNERABLE TO REMOTE CODE EXECUTION.
EXTREMESECURITY	CUSTOM ACTION SCRIPTS	IJ01043**	THE EXTREMESECURITY USER INTERFACE CAN BECOME UNRESPONSIVE WHEN LOADING THE LOG SOURCES WINDOW DUE TO A SENSORDEVICE TABLE LOCK
EXTREMESECURITY	CUSTOM ACTION SCRIPTS	IV86075**	A CUSTOM ACTION SCRIPT USING THE PARAMETER 'CREEVENTLIST' CAN FAIL AND GENERATE AN EXCEPTION IN QRADAR LOGGING
EXTREMESECURITY	CUSTOM ACTION SCRIPTS	IV86611	CUSTOM ACTION RESPONSE RETURNS 'NULL' VALUE FOR SOME DEFINED PARAMETERS
EXTREMESECURITY	ASSETS	IV89590**	THE 'ASSET NAME' FIELD FOR ASSETS CAN SOMETIMES BE BLANK
EXTREMESECURITY	UPGRADES	IV91296	PATCHING TO EXTREMESECURITY VERSION V7.7.2.7 CAN FAIL IF THE CONSOLE DATABASE HAD PREVIOUSLY BEEN MANUALLY RESTORED
Extreme Security Incident Forensics	NOTIFICATIONS	IV91662	EXTREMESECURITY SYSTEM NOTIFICATIONS SIMILAR TO '...FORENSICSNODE. FORENSICSNODE123 HAS FAILED TO START FOR XXXXX INTERVALS...'
EXTREMESECURITY	OFFENSES	IV93254	'DEVICE STOPPED SENDING EVENTS' RULE SOMETIMES DOES NOT DISPLAY THE ASSOCIATED LOG SOURCE WHEN PART OF AN OFFENSE
EXTREMESECURITY	DASHBOARD	IV93409	NEW EXTREMESECURITY USERS THAT ARE CREATED BY LDAP AUTHENTICATION DO NOT HAVE ANY DEFAULT DASHBOARDS
EXTREMESECURITY	DSM EDITOR	IV93696	DSM EDITOR CAN DISPLAY REGEX GRABS INCONSISTENTLY BETWEEN WORKSPACE FIELD AND LOG ACTIVITY PREVIEW
EXTREMESECURITY	ASSET DETAILS	IV93867**	THE ASSET DETAILS, ASSET SUMMARY WINDOW OF AN ASSET CAN SOMETIMES BE MISSING THE 'OPERATING SYSTEM' DATA
EXTREMESECURITY	OFFENSE/DSM EDITOR	IV94165	EVENTS CONTRIBUTING TO AN OFFENSE CANNOT BE DISPLAYED AFTER CUSTOM EVENT PROPERTY 'OFFENSEID' IS CREATED IN DSM EDITOR
EXTREMESECURITY	FLOWS	IV94791	FLOWSOURCE_ALIAS TABLE IS NOT REPLICATED FROM CONSOLE TO MANAGED HOSTS
EXTREMESECURITY	DSM EDITOR	IV95514	SELECTED EVENT DOES NOT DISPLAY IN THE DSM EDITOR WORKSPACE

Table 3: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 10 (continued)

Product	Component	Number	Description
EXTREMESECURITY	SEARCHES	IV96161	SEARCHES CAN FAIL WITH 'CONNECTING TO THE QUERY SERVER' ERRORS OR 'I/O ERROR OCCURRED' WHEN A LARGE NUMBER OF SECURITY PROFILES EXIST
EXTREMESECURITY	SERVICES	IV96190**	HOSTCONTEXT CAN RUN OUT OF MEMORY DUE TO TASK MANAGEMENT DATABASE TABLE BECOMING CORRUPTED
EXTREMESECURITY	DISK SPACE	IV96323	THE /STORE/TRANSIENT PARTITION DOES NOT PERFORM REQUIRED CLEANUP WHEN RUNNING LOW ON FREE DISK SPACE
EXTREMESECURITY	DISK SPACE	IV96357	/VAR/LOG/ PARTITION CAN RUN OUT OF SPACE DUE TO LOGS FILLING WITH MESSAGES 'THE USERSESSION OBJECT IN SESSIONCONTEXT...'
EXTREMESECURITY VULNERABILITY MANAGER	SEARCHES	IV96411	SEARCHES FOR VULNERABILITY BY INSTANCE CAN DISPLAY A COUNT, BUT NO DATA
EXTREMESECURITY	MASTER CONSOLE	IV96863	VIEWING OFFENSES IN MASTER CONSOLE CAN GENERATE THE ERROR 'ERROR 12: ENDPOINT INVOCATION RETURNED AN UNEXPECTED ERROR'
EXTREMESECURITY	SEARCHES	IV97167	SEARCHES CAN FAIL/CANCEL WHEN A MAXIMUM NUMBER OF RESULTS IS REACHED
EXTREMESECURITY	USER INTERFACE	IV97182	"MANAGE SEARCH RESULTS" PAGE FAILS TO LOAD WITH A 'GENERAL FAILURE. PLEASE TRY AGAIN' ERROR MESSAGE
EXTREMESECURITY	FLOW DATA	IV97276	THE QFlow PROCESS CAN SOMETIMES STOP PROCESSING WHEN OVERFLOW CONDITIONS ARE EXPERIENCED
EXTREMESECURITY	BACKUP / RESTORE	IV97342	EXTREMESECURITY BACKUPS CAN TIMEOUT WHEN APPS ARE INSTALLED
EXTREMESECURITY	LICENSE	IV97521	UNABLE TO ALLOCATE LICENSE TO A 3129 CONSOLE APPLIANCE
EXTREMESECURITY	REPORTS	IV97575	A VULNERABILITY REPORT'S VULNERABILITY COUNT VALUE CAN VARY WITHIN DIFFERENT SECTIONS OF THE SAME REPORT
EXTREMESECURITY	DEPLOYMENT	IV97835	TUNNEL CONNECTIONS REMAIN AFTER A DATA NODE OR EVENT COLLECTOR ARE REMOVED FROM A EXTREMESECURITY DEPLOYMENT
EXTREMESECURITY	FLOW DATA	IV97942	AUTO UPDATE CAN CAUSE AN INTERRUPTION IN FLOW COLLECTION AND A "PERFORMANCE DEGRADATION" SYSTEM NOTIFICATION IN THE USER INTERFACE
EXTREMESECURITY	SEARCHES	IV98068	IN PROGRESS SEARCHES THAT RUN LONGER THAN THE CONFIGURED SEARCH RESULTS RETENTION PERIOD ARE DELETED PRIOR TO COMPLETION

Table 3: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 10 (continued)

Product	Component	Number	Description
EXTREMESECURITY	DATA OBFUSCATION	IV98095	ATTEMPTING TO OBFUSCATE A LARGE VOLUME OF USERNAME FIELD BASED EVENTS CAN CAUSE OBFUSCATED EVENTS TO BE DROPPED
EXTREMESECURITY VULNERABILITY MANAGER	SCANNING	IV98207	QVM SCAN RESULT DISPLAYS 100% PROGRESS AND STOPPED AS SCAN DURATION TIME CONTINUES TO INCREMENT
EXTREMESECURITY	USER MANAGEMENT	IV98259	THE USER MANAGEMENT > AUTHENTICATION WINDOW CAN DISPLAY 'KEY NOT FOUND: JSP.EXTREMESECURITY...' MESSAGES IN THE USER INTERFACE
EXTREMESECURITY	API	IV98260	API SEARCHES RETRIEVING A COMPLETED SEARCH FROM THE /ARIEL/SEARCHES ENDPOINT CAN SOMETIMES RETURN A 500 ERROR CODE
EXTREMESECURITY	OPERATING SYSTEM	IV98442	EXTREMESECURITY V7.7.2.8 REPLACES REDHAT'S GRUB WITH GRUB 2
EXTREMESECURITY	APPLICATION FRAMEWORK	IV98486	EXTREMESECURITY APPLICAION DATA CAN APPEAR TO BE MISSING AFTER APPLYING A EXTREMESECURITY PATCH
EXTREMESECURITY	UPGRADES	IV98518	EXTREMESECURITY PATCHING TO 7.2.8P7, P8 or P9 FAILS IF THE SYSTEM WAS BUILT USING EXTREMESECURITY ISO VERSION 7.1.0.380596 AND HAS QRM
EXTREMESECURITY VULNERABILITY MANAGER	REPORTS	IV98524	EMAILED VULNERABILITY SCAN REPORTS CAN SOMETIMES BE BLANK
Extreme Security Incident Forensics	REPORTS	IV98529	QNI ONLY GENERATES FILE INFORMATION FOR THE LAST FILE CONTAINED WITHIN A SINGLE EMAIL, NOT ALL FILES
EXTREMESECURITY	SEARCH PERFORMANCE	IV98539	ARIEL SEARCHES THAT DO MANY STRING COMPARISONS CAN RUN SLOWER THAN EXPECTED IN LOW MEMORY SCENARIOS
EXTREMESECURITY	QFLOW SERVICES	IV98542	Extreme Security QFlow Collectors CAN EXPERIENCE REPETITIVE PROCESS FAILURES TO START, AND CORE DUMPS THAT CAN LEAD TO FILE SPACE ISSUES
EXTREMESECURITY VULNERABILITY MANAGER	ASSET DATA	IV98728	SCAN RESULT DATA CAN SOMETIMES FAIL TO UPDATE THE EXTREMESECURITY ASSET MODEL
EXTREMESECURITY LOG MANAGER	RULES	IV98928	ADDITIONAL RULE TESTS CANNOT BE ADDED TO CURRENT RULES AND NEW RULES CANNOT BE CREATED WHEN USING EXTREMESECURITY LOG MANAGER
EXTREMESECURITY	QUICK SEARCH INDEXES	IV99204	LUCENE INDEX DIRECTORIES DO NOT HONOR THE 'PAYLOAD INDEX RETENTION' CONFIGURED IN THE SYSTEM SETTINGS

Table 3: Issues resolved in ExtremeSecurity V7.7.2.8 Patch 10 (continued)

Product	Component	Number	Description
EXTREMESECURITY	UPGRADES	IV99289	EXTREMESECURITY MEMORY CHECK PRETEST ON AN XX48 CAN FAIL WITH A RAM REQUIREMENT ERROR '...WE NEED AT LEAST 256G OF RAM...'
EXTREMESECURITY VULNERABILITY MANAGER	SCAN RESULTS	IV99333	INCONSISTENT ASSET COUNTS WHEN DRILLING DOWN INTO SOME SCAN RESULTS
EXTREMESECURITY	UPGRADES	IV99559	EXTREMESECURITY UPGRADE FROM V7.7.2.8 P6 TO V7.7.3.0 GA CAN FAIL AT TOMCAT NOT STARTING

4 Release Notes for ExtremeSecurity V7.7.2.8 Patch 9

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 9.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

ExtremeSecurity V7.7.2.8 Patch 9 is released and resolves 1 field issues reported from users and administrators. If you already installed ExtremeSecurity V7.7.2.8 Patch 8 Interim Fix 01, there is no need to install this update as there are no new resolved issues. This release follows up V7.7.2.8 Patch 8 Interim Fix 01 for customers who are not yet on V7.7.2.8 Patch 8 to prevent them from installing both Patch 8 and an interim fix.

Before installing this update, there are three important changes that administrators should be aware of if they did not install the previous ExtremeSecurity release (V7.7.2.8 Patch 7). This message is being included in the V7.7.2.8 Patch 9 release notes for visibility:

- TLSv1 is disabled in ExtremeSecurity V7.7.2.8 Patch 7 and above. This change was originally completed in ExtremeSecurity V7.7.3.0 and has been ported to the ExtremeSecurity V7.7.2.8 software stream as of V7.7.2.8 Patch 7. This means that Tomcat will no longer listen and actively refuse browser connections using TLSv1.0 after updating to ExtremeSecurity V7.7.2.8 Patch 9. Browsers will be required to use TLSv1.1 or TLSv1.2 to authenticate to ExtremeSecurity SIEM. This should only impact users with older or legacy browsers.
- The installation of ExtremeSecurity V7.7.2.8 Patch 9 and later updates the Java version to Java 8. This change was released as part of V7.7.2.8 Patch 7, but is also being noted for administrators in the release notes for V7.7.2.8 Patch 9 to ensure this change is communicated.
- The Master Console v0.10.0 or v0.11.0 is not supported on ExtremeSecurity V7.7.2.8 Patch 7, ExtremeSecurity V7.7.2.8 Patch 8, or ExtremeSecurity V7.7.2.8 Patch 9 due to changes made with Java 8 and TLSv1.0 connections as described above. Administrators who require the Master Console should not upgrade to a version above ExtremeSecurity V7.7.2.8 Patch 6.

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRSIEM-20170726184122 to upgrade to ExtremeSecurity V7.7.2.8 Patch 9:

Current ExtremeSecurity Version	Upgrades to ExtremeSecurity V7.7.2.8 Patch 9?
ExtremeSecurity V7.7.2.3 (any patch level) or earlier	No, a minimum of ExtremeSecurity V7.7.2.4 is required.
ExtremeSecurity V7.7.2.4 (any patch level)	Yes
ExtremeSecurity V7.7.2.5 (any patch level)	Yes

Current ExtremeSecurity Version	Upgrades to ExtremeSecurity V7.7.2.8 Patch 9?
ExtremeSecurity V7.7.2.6 (any patch level)	Yes
ExtremeSecurity V7.7.2.7 (any patch level)	Yes
ExtremeSecurity V7.7.2.8 (any patch level)	Yes

The 7.2.8-QRADAR-QRSIEM-20170726184122 fix pack can upgrade ExtremeSecurity V7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for QRadar. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than ExtremeSecurity V7.7.2.4, you must upgrade to ExtremeSecurity V7.7.2.4 before proceeding to ExtremeSecurity V7.7.2.8.

Note

A ExtremeSecurity V7.7.2.8 ISO is available on IBM Fix Central for administrators to want to install a new appliance or virtual machine. Administrators who want to complete a new install need to review the *ExtremeSecurity Installation Guide*.

Resolved issues

Note

Some APAR links in the table below might take 24 hours to display properly after a software release.

Product	Component	Number	Description
EXTREMESECURITY	USER INTERFACE	IV98386	LOG SOURCE USER INTERFACE EDITS DO NOT SAVE ENABLED, COALESCING EVENTS, STORE EVENT PAYLOAD, AND GROUP ASSIGNMENT CHECK BOX ACTIONS

5 Release Notes for ExtremeSecurity V7.7.2.8 Patch 7

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 7.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

ExtremeSecurity V7.7.2.8 Patch 7 resolves 17 field issues reported from users and administrators. Before installing this update, there are important several changes that administrators should be aware of:

- TLSv1 is disabled in ExtremeSecurity V7.7.2.8 Patch 7. This change was originally completed in QRadar 7.3.0 and has been ported to the ExtremeSecurity V7.7.2.8 software stream as of V7.7.2.8 Patch 7. This means that Tomcat will no longer listen and actively refuse browser connections using TLSv1.0 after updating to ExtremeSecurity V7.7.2.8 Patch 7. Browsers will be required to use TLSv1.1 or TLSv1.2 to authenticate to ExtremeSecurity SIEM. This should only impact users with older or legacy browsers.
- The installation of ExtremeSecurity V7.7.2.8 Patch 7 updates the Java version to Java 8.
- The Master Console v0.10.0 or v0.11.0 is not supported on ExtremeSecurity V7.7.2.8 Patch 7, ExtremeSecurity V7.7.2.8 Patch 8, or ExtremeSecurity V7.7.2.8 Patch 9 due to changes made with Java 8 and TLSv1.0 connections as described above. Administrators who require the Master Console should not upgrade to a version above ExtremeSecurity V7.7.2.8 Patch 6.

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRSIEM-20170530170730 to upgrade to ExtremeSecurity V7.7.2.8 Patch 7.

Note
The 7.2.8-QRADAR-QRSIEM-20170530170730 fix pack can upgrade ExtremeSecurity 7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for ExtremeSecurity. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than 7.7.2.4, you must upgrade to 7.7.2.4 before proceeding to 7.7.2.8.

Note
A ExtremeSecurity V7.7.2.8 ISO is available on IBM Fix Central for administrators who to want to install a new appliance or virtual machine. Administrators who want to complete a new install need to review the *ExtremeSecurity Installation Guide*.

Resolved Issues

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Number	Description
SECURITY BULLETIN	IBM JAVA AS USED IN IBM EXTREMESECURITY SIEM IS VULNERABLE TO MULTIPLE CVES
IV84643	USERNAMES CONTAINING A ' . ' ARE TRUNCATED IN USER LOGINSIM AUDIT-2 EVENTS
IV86288	SOME EXTREMESECURITY SERVICES CAN FAIL TO START AFTER A 'DEPLOY FULL CONFIGURATION' IS PERFORMED
IV87510	REALTIME STREAMING CAN FAIL TO DISPLAY EVENTS WHEN FILTERING ON EVENTPROCESSOR
IV90889	DASHBOARD ITEM CAN SOMETIMES DISPLAY NO DATA IN SOME INSTANCES OF NETWORK HIERARCHY CONTAINING DOUBLE BYTE CHARACTERS
IV93256	EXTREMESECURITY RISK MANAGER PATH SEARCH CAN FAIL TO COMPLETE WHEN A SOURCEFIRE IPS EXISTS IN THE TOPOLOGY
IV93607	EXTREMESECURITY HOSTS RUNNING ON AMAZON WEB SERVICES (AWS) CAN FAIL TO UPGRADE TO QRADAR 7.2.8 DUE TO A MISSING DEPENDENCY
IV93948	'GENERAL FAILURE' ERROR WHEN PERFORMING SEARCHES AGAINST NUMERIC REFERENCE SET DATA
IV94508	POSTGRES DEADLOCKS CAN SOMETIMES LEAD TO SEARCH DATA RESULT INCONSISTENCY
IV94511	CONTENT PACK INSTALLATION CONTAINING SENSORPROTOCOLS CAN FAIL IF THE ID IS ALREADY IN THE SENSORPROTOCOL TABLE
IV94782	EXTREMESECURITY LOGGING REPORTS HOSTCONTEXT '...TOO MANY OPEN FILES' MESSAGES
IV94873	FLOW COLLECTOR APPLIANCES (12XX/13XX) WITH MULTI-THREADING ENABLED CAN STOP COLLECTING FLOWS AFTER PATCHING
IV95105	REPORTS CREATED FROM VULNERABILITY SCAN PROFILES CAN SOMETIMES BE BLANK
IV95106	REPORT DATA CAN DIFFER FROM SEARCH DATA DUE TO ACCUMULATOR ROLLUP FAILURE
IV95109	DSM EDITOR PREVIEW FUNCTION DOES NOT DISPLAY WHEN USING JAPANESE LOCALE
IV95242	PERFORMING A 'PATCH ALL' CAN DISPLAY MESSAGE 'THE FOLLOWING MANAGED HOSTS ARE NOT ACCESSIBLE VIA SSH...'
IV96155	NETWORK ACTIVITY EXPORT CAN FAIL WTIH ERROR 'THERE WAS A PROBLEM COMPLETING YOUR REPORT. PLEASE TRY AGAIN LATER.'
IV96294	EXTREMESECURITY NETWORK INSIGHT APPLIANCE NETWORK INTERFACE(S) CAN FAIL TO START/LOAD

6 Release Notes for ExtremeSecurity V7.7.2.8 Patch 6

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 6.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

ExtremeSecurity V7.7.2.8 Patch 6 resolves 26 field issues reported from users and administrators. Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRSIEM-20170403173410 to upgrade to ExtremeSecurity 7.2.8 Patch 6.

Note
The 7.2.8-QRADAR-QRFULL-20170403173410 fix pack can upgrade ExtremeSecurity 7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for ExtremeSecurity. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than 7.7.2.4, you must upgrade to 7.7.2.4 before proceeding to 7.7.2.8.

Resolved Issues

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Number	Description
IV94880	CONTENT MANAGEMENT TOOL IMPORT CAN SOMETIMES CAUSE OFFENSES TO STOP GENERATING
IV94149	EXTREMESECURITY PATCHING PROCESS CAN HANG FOR AN EXTENDED PERIOD OF TIME (HOURS) AT 'DUPLICATE REFERENCE DATA DETECTED. DELETING...'
IV93940	WHEN USING THE DSM EDITOR TO MAP EVENTS TO A CUSTOM QID, SUBSEQUENT MAPPING EVENT NAME IS 'UNKNOWN GENERIC EVENT'
IV93533	'SEND TO FORWARDING DESTINATIONS' OPTION FOR AN 'OFFENSE RULE' DISPLAYS NO AVAILABLE FORWARDING OPTIONS
IV93530	REPORTS BASED ON ADVANCED SEARCHES (AQL) THAT CONTAIN 'AS' DO NOT HAVE THE PROPER NAMED COLUMN HEADINGS

Number	Description
IV93454	AUDIT LOGGING DATA NOT AVAILABLE FOR Extreme Security Vulnerability Manager SCAN PARAMETER AND SCHEDULED TIME CHANGES
IV93205	SCAN REPORTS NOT DISPLAYING IN THE LIST OF 'AVAILABLE REPORTS' WINDOW TO EMAIL AND CAUSING NULLPOINTER EXCEPTION
IV93191	REPORTS USING ADVANCED SEARCHES (AQL) CAN SOMETIMES HAVE INCORRECT AND/OR MISSING COLUMN HEADERS
IV93146	Extreme Security Vulnerability Manager SCAN EXCLUSION SCREEN CAN SOMETIMES NOT LOAD, DISPLAYS AS A BLANK USER INTERFACE
IV93082	CSV OR XML EXPORT OF 'SCAN RESULT POLICY CHECK' SCREEN FAILS WITH ERROR 'THERE WAS A PROBLEM COMPLETING YOUR EXPORT...'
IV92977	VULNERABILITY SEARCH DASHBOARD ITEMS CHANGES DO NOT PERSIST AFTER LOG OUT OF THE EXTREMESECURITY USER INTERFACE
IV92967	QUARTZ SCHEDULING LIBRARY INFORMATION MESSAGES ARE BEING WRITTEN INTO EXTREMESECURITY LOGGING
IV92788	'AN ERROR OCCURED' POP UP MESSAGE CAN APPEAR WHEN NAVIGATING IN THE VULNERABILITIES TAB IN THE EXTREMESECURITY USER INTERFACE
IV91674	SEARCHES USING A GEOGRAPHIC LOCATION FILTER CAN RETURN UNEXPECTED RESULTS
IV91607	'UNEXPECTED ERROR WHILE RETRIEVING GET_LOGS STATUS' WHEN A NON-ADMIN USER ACCESSES SYSTEM AND LICENCE MANAGEMENT
IV91286	TIMES SERIES NOT GENERATED FOR AQL SEARCHES CONTAINING MATHEMATICAL EXPRESSIONS
IV91098	INVAILD SUPER INDEXES CAN CAUSE 'GENERAL FAILURE. PLEASE TRY AGAIN' MESSAGES WHEN USED IN A FILTER IN SEARCHES
IV90792	USERS WITH DEFAULT DOMAIN PERMISSIONS CANNOT VIEW LOG SOURCE AND LOG SOURCE GROUP EVENT FILTERS
IV90305	REQUIRE UPDATED PACKAGE TO ADDRESS TURKEY'S DECISION TO NO LONGER ADJUST CLOCKS FOR DST
IV90000	THE /VAR/LOG/QRADAR-SQL.LOG FILE DOES NOT PROPERLY ROTATE AND/OR CAN BE TRUNCATED
IV89672	LDAP HOVER TEXT TOOLTIP DISPLAYS DUPLICATE VALUES
IV89309	SORT ON 'COUNT DESCENDING' ORDERING NOT WORKING AS EXPECTED IN REPORT OUTPUT
IV88334	LOG SOURCE REPORTS CAN FAIL AND DISPLAY NO RESULTS
IV88325	REPORT WIZARD CAN HANG WHEN CREATING A LOG SOURCE REPORT
IV87964	EXTREMESECURITY APPLICATIONS USE THE CONSOLE'S PUBLIC IP IN NAT'D ENVIRONMENTS
IV87497	VULNERABILITY SEARCH DASHBOARD ITEMS CHANGES DO NOT PERSIST AFTER LOG OUT OF THE EXTREMESECURITY USER INTERFACE

7 Release Notes for ExtremeSecurity V7.7.2.8 Patch 4

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 4.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. There are five APARs associated with ExtremeSecurity V7.7.2.8 Patch 4, which address a number of specific issues in ExtremeSecurity V7.7.2.8. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRFULL-20170224202650 to upgrade to ExtremeSecurity 7.7.2.8 Patch 4:

Note
The 7.2.8-QRADAR-QRFULL-20170224202650 fix pack can upgrade ExtremeSecurity 7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for ExtremeSecurity. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than 7.7.2.4, you must upgrade to 7.7.2.4 before proceeding to 7.7.2.8.

Resolved Issues

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Number	Description
SECURITY BULLETIN	Extreme SIEM IS VULNERABLE TO A DENIAL OF SERVICE (CVE-2016-9740)
SECURITY BULLETIN	Extreme SIEM AND Extreme Security Incident Forensics ARE VULNERABLE TO CROSS-SITE REQUEST FORGERY (CVE-2016-9730)
SECURITY BULLETIN	Extreme SIEM IS VULNERABLE TO MISSING AUTHENTICATION CHECKS (CVE-2016-9729)
SECURITY BULLETIN	Extreme SIEM AND Extreme Security Incident Forensics ARE VULNERABLE TO OS COMMAND INJECTION (CVE-2016-9726, CVE-2016-9727)
SECURITY BULLETIN	Extreme SIEM IS VULNERABLE TO SQL INJECTION (CVE-2016-9728)

Number	Description
SECURITY BULLETIN	Extreme Security Incident Forensics IS VULNERABLE TO OVERLY PERMISSIVE CORS ACCESS POLICIES (CVE-2016-9725)
SECURITY BULLETIN	Extreme SIEM IS VULNERABLE TO XML ENTITY INJECTION (CVE-2016-9724)
SECURITY BULLETIN	Extreme SIEM AND QRADAR Extreme Security Incident Forensics ARE VULNERABLE TO CROSS SITE SCRIPTING (CVE-2016-9723, CVE-2017-1133)
SECURITY BULLETIN	Extreme SIEM AND Extreme Security Incident Forensics ARE VULNERABLE TO INFORMATION EXPOSURE (CVE-2016-9720)
SECURITY BULLETIN	MOZILLA NSS AS USED IN Extreme SIEM IS VULNERABLE TO ARBITRARY CODE EXECUTION (CVE-2016-2834)
SECURITY BULLETIN	PIVOTAL SPRING FRAMEWORK AS USED IN Extreme SIEM IS VULNERABLE TO VARIOUS CVEs
SECURITY BULLETIN	APACHE SOLR AS USED IN Extreme SIEM AND Extreme Security Incident Forensics IS VULNERABLE TO A DENIAL OF SERVICE
SECURITY BULLETIN	Extreme SIEM CONTAINS HARD-CODED CREDENTIALS
SECURITY BULLETIN	Extreme SIEM USES BROKEN OR RISKY CRYPTOGRAPHIC ALGORITHMS
SECURITY BULLETIN	APACHE TOMCAT PRIOR TO VERSION 6.0.48 IS SUSCEPTIBLE TO SEVERAL VULNERABILITIES
SECURITY BULLETIN	Extreme SIEM AND Extreme Security Incident Forensics ARE VULNERABLE TO VARIOUS CVEs FOUND IN IBM JAVA.
SECURITY BULLETIN	OPENSSL AS USED IN Extreme SIEM IS VULNERABLE TO VARIOUS CVEs
IV86405	'APPLICATION ERROR' WHEN USING A VALUE SPECIFIED IN 'AS' CLAUSE FOR LOGSOURCENAME IN AN ADVANCED SEARCH (AQL)
IV86407	THE /VAR/LOG PARTITION CAN FILL DUE TO THE EXTREMESECURITY LOG FILES BEING QUICKLY FILLED WITH 'EXCEPTION IN TEST' MESSAGES
IV87313	'SOURCE' AND 'DESTINATION' NETWORK GROUP SHOW FULL NETWORK HIERARCHY NAME WHEN ADDED AS A COLUMN TO DISPLAY
IV87507	SOME DASBOARD ITEMS NO LONGER DISPLAY IN THE EXTREMESECURITY USER INTERFACE
IV87862	RULE 'EXPLOIT: DESTINATION VULNERABLE TO DETECTED EXPLOIT' CAN SOMETIMES NOT TRIGGER WHEN EXPECTED
IV89015	APPLICATION ERROR WHEN DOUBLE CLICKING THE RESULTS OF AN 'ADVANCED SEARCH' (AQL)
IV89556	ECS-EP PROCESS RUNNING, BUT EVENT/FLOW PROCESSING NOT OCCURING ON A EXTREMESECURITY APPLIANCE
IV89820	SYSLOG EVENTS GENERATED FROM AN OFFENSE RULE DO NOT CONTAIN ANY CONFIGURED NAMING CONTIBUTIONS IN THE EVENT PAYLOAD
IV89893	'ASSET MODEL HAS NOT YET BEEN UPDATED WITH SCAN RESULTS' MESSAGE WHEN NO ASSETS HAVE BEEN SCANNED
IV89904	VULNERABILITY MANAGER EXCEPTIONS FOR IP/CIDR/NETWORK ARE NOT RESPECTED WHEN A FILTER IS DEFINED TO EXCLUDE THEM

Number	Description
IV89929	'MISSING PATCHES' REPORT CAN SOMETIMES BE EMPTY WHEN RUN ON SYSTEMS WITH A LARGE NUMBER OF VULNERABILITY INSTANCES
IV90002	VULNERABILITY MANAGER RED WARNING TRIANGLE DISPLAYED ON A SCAN RESULT WHEN THE ASSET MODEL WAS PROPERLY UPDATED
IV90004	ASSET MODEL 'NOT UPDATED' ICON DISPLAYS FOR A SCAN PROFILE RESULT WHEN SCAN POLICY HAS BEEN EDITED
IV90075	RED WARNING ICON ON VULNERABILITY MANAGER SCAN RESULTS PAGE WHEN RESULTS HAVE BEEN REPUBLISHED
IV90376	SECURITY APP EXCHANGE APPLICATIONS CAN FAIL TO COMMUNICATE IN SOME HIGH AVAILABILITY EXTREMESECURITY CONFIGURATIONS
IV90421	RULE TESTS AGAINST A REFERENCE MAP DO NOT WORK WHEN DESTINATION PORT IS NULL
IV90793	PATCHING TO EXTREMESECURITY 7.2.8 GA OVERWRITES CA CERTS THAT WERE LOCATED IN /ETC/PKI/TLS/CERTS/CA-CUNDLE.CRT
IV90795	DRILLING INTO A SEARCH THAT WAS GROUPED BY A CUSTOM EVENT PROPERTY WITH PARENTHESIS DOES NOT WORK AS EXPECTED
IV90887	'ASSET MODEL HAS NOT YET BEEN UPDATED WITH SCAN RESULTS' MESSAGED DISPLAYED WHEN ASSET MODEL IS UPDATED CORRECTLY
IV90906	TIMES SERIES NOT WORKING FOR SOME NON-ADMIN EXTREMESECURITY USERS
IV91300	CREATING A REPORT BASED ON AN AQL (ADVANCED SEARCH) QUERY CONTAINING 'ORDER BY' FAILS TO GENERATE PROPER OUTPUT
IV91322	ATTEMPTING TO ENABLE TIMESERIES COLLECTION FOR SHARED SAVED SEARCHES CAN SOMETIMES FAIL
IV91615	'ERROR: COULD NOT FIND OR LOAD MAIN CLASS COM.Q1LABS.CORE.UTIL . PASSWORDENCRYPT' WHEN CONFIGURING LDAP HOVER FEATURE
IV91618	EDIT SEARCH PAGE CAN SOMETIMES FAIL TO LOAD ALL OF THE EXPECTED SEARCH PAGE OPTIONS
IV91634	ARIEL SEARCHES THAT ARE RUN USING API VERSION 7.0+ DO NOT RETURN PAYLOAD PROPERLY FOR PARSING
IV91635	QUICK SEARCHES CANNOT BE REMOVED FROM THE QUICK SEARCH LIST
IV91675	AN 'APPLICATION ERROR' CAN BE DISPLAYED FOR NEW USERS LOGGING INTO THE QRADAR USER INTERFACE INSTEAD OF A DEFAULT DASHBOARD
IV91816	PATCHING EXTREMESECURITY HIGH AVAILABILITY (HA) PAIR APPLIANCES CONFIGURED USING CROSSOVER CAN SOMETIMES FAIL
IV92139	'WRAP TEXT' FUNCTION FOR EVENT PAYLOAD INFORMATION DOES NOT WORK AFTER APPLYING EXTREMESECURITY PATCH
IV92466	EXTREMESECURITY SEARCHES CAN FAIL TO COMPLETE AND/OR DASHBOARD DATA CAN FAIL TO LOAD DUE TO AN ARIEL CONNECTION LEAK

Number	Description
IV92851	ARIEL CAN BECOME OVERLOADED CAUSING SLOWER THAN EXPECTED SEARCH RESULTS AND SLOW USER INTERFACE RESPONSE
IV92852	REPORTS RUNNING ON 'ACCUMULATED DATA' CAN SOMETIMES FAIL DUE TO THE GLOBAL VIEW DAILY ROLLUPS FAILING
IV93839	EXTREMESECURITY FEATURES USING THE ARIEL PROCESS (SEARCHES, DASHBOARDS, REPORTS, ETC.) CAN INTERMITTENTLY FAIL TO LOAD/ COMPLETE (NOTE: THIS APAR WAS RECENTLY ADDED AND MIGHT TAKE UP TO 12 HORUS TO DISPLAY)

8 Release Notes for ExtremeSecurity V7.7.2.8 Patch 3

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 3.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. There are five APARs associated with ExtremeSecurity V7.7.2.8 Patch 3, which address a number of specific issues in ExtremeSecurity V7.7.2.8. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRFULL-20170105231716 to upgrade to ExtremeSecurity 7.7.2.8 Patch 3:

Note
The 7.2.8-QRADAR-QRFULL-20170105231716 fix pack can upgrade ExtremeSecurity 7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for ExtremeSecurity. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than 7.7.2.4, you must upgrade to 7.7.2.4 before proceeding to 7.7.2.8.

Resolved Issues

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Number	Description
IV89519	RULES THAT TEST AGAINST REFERENCE MAP OF DATA SETS CAN SOMETIMES FIRE UNEXPECTEDLY
IV89901	EXTREMESECURITY AUTO UPDATE FEATURE CONFIGURED TO USE A PROXY SERVER CAN FAIL AFTER PATCHING
IV91030	EXTREMESECURITY APPS THAT REQUIRE SPECIFIC USER ROLE PERMISSIONS CAN STOP WORKING AFTER PATCHING TO EXTREMESECURITY 7.2.8 PATCH 1
IV91617	QFLOW APPLIANCES CAN STOP SENDING FLOWS TO FLOW PROCESSORS AFTER PATCHING TO EXTREMESECURITY 7.2.8
IV92220	TIME SERIES DATA ACCUMULATION DOES NOT WORK FOR NON-ADMIN DOMAIN USERS WITH MULTI-TENANCY DASHBOARD

9 Release Notes for ExtremeSecurity V7.7.2.8 Patch 1

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.8 Patch 1.

Note
We recommend that you review this document prior to installing or upgrading this product.

About this Patch

Fix packs are cumulative software updates to fix known software issues in your ExtremeSecurity deployment. ExtremeSecurity fix packs are installed by using an SFS file. The fix pack can update all appliances attached to the ExtremeSecurity Console. If your deployment is installed with any of the following ExtremeSecurity versions, you can install fix pack 7.2.8-QRADAR-QRFULL-20161118202122 to upgrade to ExtremeSecurity 7.7.2.8:

Note
The 7.2.8-QRADAR-QRFULL-20161118202122 fix pack can upgrade ExtremeSecurity 7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for ExtremeSecurity. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than 7.7.2.4, you must upgrade to 7.7.2.4 before proceeding to 7.7.2.8.

Resolved Issues

Note
Some APAR links in the table below might take 24 hours to display properly after a software release.

Number	Description
IV77767	EXTREMESECURITY USER INTERFACE OUTAGES CAN OCCUR WHEN TRYING TO LOAD THE MANAGED SEARCH RESULTS PAGE
IV83509	USING 'WHEN THE EVENT(S) HAVE NOT BEEN DETECTED...' RULE WITH A RESPONSE TO CREATE NEW EVENT, THAT EVENT HAS INCORRECT QID
IV83701	ERRORS VISIBLE IN EXTREMESECURITY LOGGING AFTER A CUSTOM EVENT PROPERTY HAS BEEN SUCCESSFULLY DELETED
IV84025	UNABLE TO DELETE RULES THAT ARE ADDED TO THE GROUP 'ANOMALY'
IV84615	RULE OR BUILDING BLOCK DELETION CAN FAIL WHEN THERE ARE INVALID SEARCHES

Number	Description
IV86422	'MORE OPTIONS' IS DISPLAYED TWICE WHEN PERFORMING A RIGHT CLICK OF A SOURCE AND/OR DESTINATION IP IN A NETWORK ACTIVITY SEARCH
IV86683	THE EVENT PAYLOAD INFORMATION FIELD DOES NOT PROPERLY DISPLAY UTF DATA IF IT CONTAINS CONSECUTIVE SPACES OR A TAB CHARACTER
IV87248	HIGH AVAILABILITY CONSOLE WITH CROSSOVER CONNECTIONS CAN HANG AND/OR FAIL DURING PATCHING
IV87577	QUICK FILTER CONTAINING DOUBLE-BYTE CHARACTERS ON LOG AND/OR NETWORK ACTIVITY TAB DOES NOT WORK AS EXPECTED
IV87796	CUSTOM EVENT PROPERTIES DO NOT FORWARD THROUGH A CUSTOM RULE RESPONSE WHEN USING JSON FORMAT
IV87859	SOME LOG SOURCES CAN FAIL TO BE IMPORTED DURING A CONTENT MANAGEMENT TOOL IMPORT
IV88275	NON-ADMIN EXTREMESECURITY USERS ARE UNABLE TO FILTER ON 'EVENT PROCESSOR'
IV88279	USER ROLE WITH ONLY 'MANAGE LOG SOURCES' UNDER 'DELEGATED ADMINISTRATION' CANNOT PERFORM A DEPLOY FUNCTION
IV88324	THE SYSTEM HEATH (HEALTH CONSOLE) FEATURE CAN HAVE VARIOUS PROBLEMS AFTER APPLYING A PATCH
IV88392	ORDERING OF ASSETS BY IP ADDRESS SOMETIMES DOES NOT WORK AS EXPECTED
IV88708	VULNERABILITY MANAGER - ASSET DETAILS RISK POLICY SCREEN SHOWS INCORRECT TIMESTAMP IN LAST EVALUATED FIELD WHEN TIME ZONE IS SET FOR NEW ZEALAND
IV89064	THE EXTREMESECURITY ARIEL API CAN SOMETIMES RETURN NO RESULTS WHEN PROCESSING LARGE NUMBERS OF SEARCH RESULTS
IV89173	VULNERABILITY MANAGER - CIDR DATA ENTRY VALIDATION FOR SCANNERS DOES NOT WORK AS EXPECTED
IV89196	SEARCHING ON COMPRESSED DATA USING FILTER 'RETENTION BUCKET IS' RETURNS NO RESULTS
IV89308	THE EXTREMESECURITY RULES PAGE FAILS TO LOAD OR TAKES A LONGER THAN EXPECTED TIME TO LOAD
IV89309	SORT ON 'COUNT DESCENDING' ORDERING NOT WORKING AS EXPECTED IN REPORT OUTPUT
IV89345	VULNERABILITY MANAGER: CIS SCAN RESULT STATUS CAN SOMETIMES DISPLAY AS FAIL INSTEAD OF UNKNOWN IN THE USER INTERFACE
IV89365	VULNERABILITY MANAGER: VULNERABILITY FILTERING BY VENDOR AND DATE RANGE SOMETIMES DOES NOT RETURN THE COMPLETE LIST OF VULNERABILITIES
IV89367	EXTREMESECURITY SYSTEM NOTIFICATION: 'TRANSACTION SENTRY: RESTORED SYSTEM HEALTH BY CANCELLING HUNG TRANSACTIONS OR DEADLOCKS
IV89393	CONTENT MANAGEMENT TOOL (CMT) EXPORT OF CUSTOM RULES FAILS WITH A NULLPOINTER EXCEPTION

Number	Description
IV89408	VULNERABILITY MANAGER SCANS UNEXPECTEDLY DISPLAY A ZERO VULNERABILITY COUNT AND NO ASSETS CREATED FROM THOSE SCANS
IV89516	SAVED SEARCHES ATTEMPTING TO USE CVE-ID NUMBER DATA IN REFERENCE SETS DO NOT WORK AS EXPECTED
IV89665	FILTERING ON 'USERNAME IS ANY OF' " " (A BLANK SPACE WITHIN QUOTES) DOES NOT DISPLAY AS A CURRENTLY APPLIED FILTER
IV89901	EXTREMESECURITY AUTO UPDATE FEATURE CONFIGURED TO USE A PROXY SERVER CAN FAIL AFTER PATCHING
IV90087	SEARCHES CAN TAKE A LONGER THAT EXPECTED TIME TO COMPLETE IN 7.2.8 GA
IV90323	UNABLE TO DELETE REFERENCE SET ELEMENTS USING THE USER INTERFACE
IV90372	ATTEMPTING TO ADD AN ADVANCED SEARCH (AQL) TEST TO A RULE CAN CAUSE THE USER INTERFACE WINDOW TO BECOME UNRESPONSIVE
IV90419	EVENT DATA WRITTEN INTO EXTREMESECURITY AT VERSION 7.2.3.X OR PRIOR CANNOT BE READ BY VERSION 7.2.7.X AND 7.2.8 GA
IV90460	EXTREMESECURITY DEPLOY FUNCTION CAN FAIL AFTER PATCHING TO 7.2.8 GA
IV90646	QFLOW PROCESS CAN STOP WORKING AS EXPECTED ON FLOW APPLIANCES AFTER PATCHING TO 7.2.8 GA
IV90649	PATCH PROCESS TO 7.2.8 GA FAILS DUE TO A USER AND AUTHORIZED SERVICE HAVING THE SAME NAME
IV90777	NO FLOWS OR EVENTS VISIBLE IN THE EXTREMESECURITY USER INTERFACE AFTER RESTORING A CONFIGURATION BACKUP FROM 7.2.8 GA

10 Release Notes for ExtremeSecurity V7.7.2.8

Introduction

Extreme Networks Security Analytics V7.7.2.8 provides new features and fixes to known issues.

The `728_QRADAR-QRFULL-20160920132350` fix pack can upgrade ExtremeSecurity V7.7.2.4 (7.2.4.983526) and later to the latest software version. However, this document does not cover all of the installation messages and requirements, such as changes to memory requirements or browser requirements for ExtremeSecurity. To review any additional requirements, see the *ExtremeSecurity Upgrade Guide*. If you are on a version of ExtremeSecurity earlier than V7.7.2.4 you must upgrade to V7.7.2.4 before proceeding to ExtremeSecurity V7.7.2.8. For more information, see the Software Upgrade Progression technical note.

Contents

New features

The following new features and improves are available after installing ExtremeSecurity V7.7.2.8.

- X-Force Threat Intelligence feed is now free and included with all QRadar appliances by enabling a system setting.
- Administrators can now manage expensive searches by setting resource restrictions on specific users.
- Data segregation: Reference sets are now domain aware and the user interface includes a domain setting.
- Event and Flow data retention buckets now support tenants.
- The offense assignment user interface as been improved and support tenants.
- Offense renaming allows offenses to be created with more useful names.
- A new DSM Editor provides a user interface to replace writing complex log source extensions for new or unknown data sources.
- Delete users from ExtremeSecurity now prompts administrators to reassign any existing content to existing users.
- ExtremeSecurity V7.7.2.8 introduces several new and updated API endpoints.
- AQL now supports nested queries (sub-queries) in advanced searches, using IN or FROM statements.

- Search performance enhancements: Asset query performance and UI wait times significantly improved.
- Vulnerability user interface query performance is significantly improved.
- Security Master Console now included with ExtremeSecurity . A separate RPM install is no longer required.

For a full list of changes, see What's new in ExtremeSecurity V7.7.2.8.

System requirements

For information about hardware and software compatibility, see the detailed system requirements in the *ExtremeSecurity Installation Guide*.

Installing ExtremeSecurity

Note
A minimum of ExtremeSecurity V7.7.2.4 is required before upgrading to V7.7.2.8.

For full installation instructions, see the *ExtremeSecurity Installation Guide*.

Fix list

Number	Description
IV81172	SQL Exception when running Events/Logs reports based on Advanced Search for assets
IV87841	Rule test with multiple reference sets only matches first reference set in test
IV82547	Web application XJAVASCRIPT filtering broken
IV84386	Critsit: Log Activity - UI Exception Popup when mousing over IP addresses
IV88370	Reference Data - Bulk Loading Performance Needs Work
IV84710	Asset screen in UI is slow when the number of assets is moderate to large
IV85584	Rule wizard UI issues
IV79236	CritSit: Cannot access Rule Wizard when navigating to an event through an offense
IV85435	Offense naming not working consistently
IV87029	Index roller bug
IV70567	Autoupdate HTTPS and proxy interception - CONNECT failures by UpdateConfs.pl
IV84567	Offenses Over Time reports can mismatch Offense Screen
IV86839	Filtering in Log Sources while sorted by EPS causes exception
IV82557	NullPointerException in Data Deletion causes user unable to delete rule or custom event property

Known Issues

Issue description	Workaround
When you install Extreme Security Incident Forensics, the Appliance ID 6200 appears as an option. This is reserved for future use.	The software will be available at a future date.