Extreme Networks Security Analytics Release Notes

For Software Version 7.7.2.7

9035016-03

Published December 2016

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

Support

For product support, including documentation, visit: http://www.extremenetworks.com/support/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Preface

Related Publications

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

ExtremeSecurity Analytics & SIEM

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

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:

- Global Technical Assistance Center (GTAC) 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.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

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 Return Material Authorization (RMA) numbers

1 About the ExtremeSecurity V7.7.2.7 Release Notes

V7.7.2.7 Firmware Releases
Patch Installation Instructions

These release notes cover ExtremeSecurity for release V7.7.2.7, including patches. These notes cover:

- Firmware support
- Fixes
- Known Issues

For the patch upgrade procedure, see Patch Installation Instructions on page 6.

V7.7.2.7 Firmware Releases

Status	Firmware Version	Product Type	Release Date
Current Version	V7.7.2.7 20161017135129	Customer Software	December 9, 2016
Previous Version	V7.7.2.7 Build 20160906164309	Customer Software	October 26, 2016
Previous Version	V7.7.2.7 Build 20160816201941	Customer Software	September 9, 2016
Previous Version	V7.7.2.7 Build 20160519230548	Customer Software	July 21, 2016

Patch Installation Instructions

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

- Back up your data before you begin any software upgrade. For more information about backup and recovery, see the *Extreme SIEM Administration Guide*.
- To avoid access errors in your log file, close all open SIEM sessions.
- The fix pack for Extreme Security 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.

Fix packs are cumulative software updates to fix known software issues in your SIEM deployment. SIEM fix packs are installed by using an SFS file. The fix pack can update any appliance attached to the SIEM Console that is at the same software version as the Console.

1. Download the `727_patchupdate-7.2.7.<build_number>.sfs` patch 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 726_patchupdate-7.2.7<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 1 Console
2 2 Event Processors
3 3 Event Collectors
4 4 Flow Processors
5 5 Flow Collectors

As of Extreme Security 7.7.2.6 Patch 3 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 Extreme Security 7.7.2.6 Patch 3 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. The Console appliance must be upgraded before you can do a local update for your managed host.

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.

At 01:00 AM appliance local time following a successful patch, all index files on an appliance that were generated while running 7.7.2.6 or 7.7.2.7 will be validated to ensure that all indexes on the appliance are accurate. This one-time validation could take several hours to complete depending on the amount of index data. The index validation process does not significantly impact the performance of other Extreme Security processes.

If the administrator wants to adjust the time at which index validation starts, they can contact Extreme support for assistance.

2 Release Notes for ExtremeSecurity V7.7.2.7 Patch 4

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.7 Patch 4.

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

If your deployment is installed with ExtremeSecurity 7.7.2.4 or later, you can install fix pack V7.7.2.7 Build 20161017135129.

Note
The 7.2.7-QRADAR-QRSIEM-20161017135129 fix pack can upgrade 7.7.2.4 to 7.7.2.6 (any patch level) and above to the latest software version. However, this document does not cover all of the installation messages and requirements. For information on upgrading from 7.2.4 or later, see the *ExtremeSecurity Upgrade Guide*.

About this Patch

ExtremeSecurity V7.7.2.7 Patch 4 resolves 11 issues reported in previous released of ExtremeSecurity V7.7.2.7. The update must be installed on the Console first, then all other appliances can be updated. Administrators can use the patch 'ALL' option to upgrade the entire deployment.

Resolved Issues

As ExtremeSecurity V7.7.2.7 Patch 4 is a cumulative release, the release notes listed below include additional tables for issues resolved in previous 7.2.7 patch updates.

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

Product	Number	Description
EXTREMESECURITY	IV89196	SEARCHING ON COMPRESSED DATA USING FILTER 'RETENTION BUCKET IS' RETURNS NO RESULTS
VULNERABILITY MANAGER	IV89408	VULNERABILITY MANAGER SCANS UNEXPECTEDLY DISPLAY A ZERO VULNERABILITY COUNT AND NO ASSETS CREATED FROM THOSE SCANS
EXTREMESECURITY	IV89516	SAVED SEARCHES ATTEMPTING TO USE CVE-ID NUMBER DATA IN REFERENCE SETS DO NOT WORK AS EXPECTED
EXTREMESECURITY	IV89363	MULTIPLE SIMULTANEOUS REFERENCE DATA ADDITIONS AND/OR DELETIONS USING THE API CAN CAUSE THE UI TO BECOME UNRESPONSIVE

Product	Number	Description
EXTREMESECURITY	IV89308	THE EXTREMESECURITY RULES PAGE FAILS TO LOAD OR TAKES A LONGER THAN EXPECTED TIME TO LOAD
EXTREMESECURITY	IV87841	RULE TEST CONTAINING 'ANY OF THESE REFENCE SET(S)' ONLY MATHCES THE FIRST REFERENCE SET DEFINED IN THE TEST
EXTREMESECURITY	IV88275	NON-ADMIN EXTREMESECURITY USERS ARE UNABLE TO FILTER ON 'EVENT PROCESSOR'
EXTREMESECURITY	IV88324	THE SYSTEM HEATH (EXTREMESECURITY HEALTH CONSOLE) FEATURE CAN HAVE VARIOUS PROBLEMS AFTER APPLYING A PATCH
VULNERABILITY MANAGER	IV89209	REPEATED ARIEL PROCESS OUT OF MEMORY OCCURANCES WITH LARGE VOLUMES OF DATA IN /STORE/TRANSIENT
EXTREMESECURITY	IV89309	SORT ON 'COUNT DESCENDING' ORDERING NOT WORKING AS EXPECTED IN REPORT OUTPUT
EXTREMESECURITY	IV87841	RULE TEST CONTAINING 'ANY OF THESE REFENCE SET(S)' ONLY MATHCES THE FIRST REFERENCE SET DEFINED IN THE TEST

3 Release Notes for ExtremeSecurity V7.7.2.7 Patch 3

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.7 Patch 3.

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

If your deployment is installed with ExtremeSecurity 7.7.2.4 or later, you can install fix pack V7.7.2.7 Build 20160906164309.

Note
The 7.2.7-QRADAR-QRSIEM-20160906164309 fix pack can upgrade 7.7.2.4 to 7.7.2.6 (any patch level) and above to the latest software version. However, this document does not cover all of the installation messages and requirements. For information on upgrading from 7.2.4 or later, see the *ExtremeSecurity Upgrade Guide*.

About this Patch

This patch resolves 14 issues reported previously in V7.7.2.7. The update must be installed on the Console first, then all other appliances can be updated. Administrators can use the patch 'ALL' option to upgrade the entire deployment.

Resolved Issues

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

Product	Number	Description
EXTREME SECURITY VULNERABILITY MANAGER	IV83769	NAVIGATING TO THE 'MY ASSIGNED VULNERABILITIES' SCREEN CAN HANG AND THE USER INTERFACE CAN BECOME INACCESSIBLE
EXTREME SECURITY	IV84648	SINGLE SHARED DASHBOARD FROM A USER ROLE DISPLAYS FOR ALL MEMBERS OF THE USER ROLE WHEN THEY LOGIN
EXTREME SECURITY	IV84681	DASHBOARD TIME SERIES CHARTS DO NOT SHOW THEIR FULL TITLE IF THE TEXT CONTAINS PARENTHESIS
EXTREME SECURITY	IV84730	A NULLPOINTER EXCEPTION MIGHT OCCUR DURING SEARCHES/REPORTS AFTER DELETING A SECURITY PROFILE THAT HAS NO ASSIGNED USERS
EXTREME SECURITY	IV85363	PERFORMING AN ASCENDING OR DESCENDING SORT OF LOG SOURCES BY 'STATUS' DOES NOT PROPERLY SORT THE ENTRIES

Product	Number	Description
EXTREME SECURITY	IV85595	'DEVICE STOPPED SENDING EVENTS' RULE DOES NOT DISPATCH A NEW EVENT
EXTREME SECURITY	IV85758	EXTREME SECURITY 'DEPLOY CHANGES' CAN SOMETIMES FAIL ON A REMOTE MANAGED HOST, WITH ENCRYPTION, AND SLOW LINK TO CONSOLE
EXTREME SECURITY	IV86076	THE ROUTING RULES OPTION 'PREFIX A SYSLOG HEADER IF IT IS MISSING OR INVALID' DOES NOT WORK FOR OFFLINE FOWARDING
EXTREME SECURITY	IV86685	REPLICATION OF RM DATA FROM CONSOLE TO MANAGED HOSTS CAN CAUSE A REPLICATION PERFORMANCE ISSUE ON MANAGED HOSTS
EXTREME SECURITY VULNERABILITY MANAGER	IV86845	'SCANS COMPLETED' VULNERABILITY MANAGEMENT DASHBOARD CAN BE SLOW OR FAIL TO LOAD
EXTREME SECURITY	IV87515	"TYPEERROR: CANNOT READ PROPERTY '1' OF UNDEFINED" WHEN ACCESSING RULES PAGE USING CHROME BROWSER VERSION 53. THIS DEFECT IS CLONED FORWARD FROM 7.2.7 PATCH 2.
EXTREME SECURITY	IV87565	XML EXPORT HAS INCORRECTLY FORMATED CDATA FIELD
EXTREME SECURITY	IV87575	CUSTOM RULE ENGINE COMMON RULE TYPES DO NOT ALWAYS DISPLAY AS OPTIONS

4 Release Notes for ExtremeSecurity V7.7.2.7 Patch 2

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.7 Patch 2.

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

If your deployment is installed with ExtremeSecurity 7.7.2.4 or later, you can install fix pack V7.7.2.7 Build 20160816201941.

Note
The 7.2.7-QRADAR-QRSIEM-20160816201941 fix pack can upgrade 7.7.2.4 to 7.7.2.6 (any patch level) and above to the latest software version. However, this document does not cover all of the installation messages and requirements. For information on upgrading from 7.2.4 or later, see the *ExtremeSecurity Upgrade Guide*.

About this Patch

ExtremeSecurity V7.7.2.7 Patch 2 is a replacement update for V7.7.2.7 Patch 1, which was removed due to APAR IV87973. Not all users will experience the issue described in IV87973, however, Patch 2 is being issued as a replacement download. This update also resolves an issue in Chrome introduced by Google in browser v52 and v53.

Resolved Issues

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

Product	Number	Description
EXTREME SECURITY	IV87973	AFTER PATCHING TO 7.7.2.7 PATCH 1, THE /VAR/LOG/ PARTITION CAN RUN OUT OF FREE SPACE, CAUSING EXTREME SECURITY SERVICES TO SHUT DOWN.
EXTREME SECURITY	IV87515	MESSAGE `TYPEERROR: CANNOT READ PROPERTY '1' OF UNDEFINED` DISPLAYS WHEN ACCESSING RULES PAGE USING CHROME BROWSER VERSION 53.

5 Release Notes for ExtremeSecurity V7.7.2.7

New Features

Descriptions of new features are available in the Knowledge Center.

System Requirements

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

Installing ExtremeSecurity

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

Fix List

Number	Description
IV50320	WinCollect agents contain a default event throttle that might not be sufficient for high EPS Windows systems.
IV67458	Rules that compare a numerically formatted custom property to a numerical reference set fail to match.
IV72794	The ExtremeSecurity/Store/Transient partition can exceed 95% disk space usage causing services to stop.
IV73253	ExtremeSecurity unable to add reference table elements when using port, IP, or numeric reference tables.
IV76726	Geographic country/region data populated into reference tables is not used consistently when testing against other rules.
IV78329	Unable to perform rule or advanced query comparisons using 'date' type reference data.
IV78720	Offenses can sometimes stop generating or updating in certain 'Flow source stopped sending flows' scenarios.
IV79198	System notifications related to 'Berkeley DB library' can sometimes be generated within ExtremeSecurity.
IV79686	No system health data is displayed after performing an ExtremeSecurity configuration restore.
IV79698	Non-admin users assigned to a domain are unable to switch report groups.
IV79930	Creating an asset manually can take a longer than expected amount of time and/or appears to hang indefinitely.
IV81997	An ariel_proxy_server 'out of memory' can sometimes occur during event and/or flow searches.

Number	Description
IV82160	Cre failed to read rules messages in ExtremeSecurity logging after performing a content management tool import.
IV83455	Data node rebalancing process can sometimes fail and restart taking a longer than expected time to rebalance.
IV83535	Report on top offenses that are based on saved searches containing domain filters do not work as expected.
IV83748	An error occurred positioning the result set returned from the server to row 1...error message displayed in search results.
IV84025	Unable to delete rules that are added to the group 'anomaly'.
IV84056	Advanced searches (AQL) that contain 'log source group' filter or column can appear to hang.
IV84062	ExtremeSecurity user interface action bar is missing from multiple UI screens.
IV84390	Error pop-up or blank window can occur when using Chrome or Internet Explorer browser in specific filter search instances.
IV84511	Unable to remove the 'Optimize parsing for rules, reports and searches' flag on custom event/flow properties.
IV84682	ExtremeSecurity vis component does not get re-added to QFlow appliance when a QFlow is removed and re-added to a deployment.
IV84689	Offline forwarding from data nodes does not work.
IV84733	ExtremeSecurity can fail to parse events that have unresolved DNS names.
IV85210	Invalid backup archive message when attempting to upload a backup file from within the ExtremeSecurity user interface.

Known Issues

Issue description	Workaround
Juniper patch - FATAL: Could not load /lib/modules/2.6.32-431.29.2.el6.x86_64/modules.dep: No such file or directory.	When the patch finishes, restart the system to load the new kernel.
Historical correlation - event profile not showing all saved searches available.	Historical correlation does not show aggregated results.
Externally-sourced geodata.conf is not accurate enough and causing false/positives in the customer environment.	The location associated with the CIDR range is the country the IP is registered in, and not the country the IP is coming from.