Extreme®
Connect Beyond the Network

Extreme Networks Security Analytics Release Notes

For Software Version 7.7.2.5

9034921-01

Published December 2015

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: www.extremenetworks.com/documentation/

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

Table of Contents

Preface **4**
Related Publications 4
Providing Feedback to Us 4
Getting Help 5

Chapter 1: About these Release Notes **6**
Product Firmware Support 6
Patch Installation Instructions 6

Chapter 2: ExtremeSecurity V7.7.2.5 Patch 6 Release Notes **9**

Chapter 3: ExtremeSecurity V7.7.2.5 Patch 5 Release Notes **10**

Chapter 4: ExtremeSecurity V7.7.2.5 Patch 4 Release Notes **13**

Chapter 5: ExtremeSecurity V7.7.2.5 Patch 3 Release Notes **16**

Chapter 6: ExtremeSecurity V7.7.2.5 Release Notes **19**
Resolved Issues 19

Preface

Related Publications

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

ExtremeSecurity Analytics

- *Extreme Security Release Notes*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Users Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*
- *Extreme Networks Security Log Manager Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security Vulnerability Assessment Configuration 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: 1-800-872-8440 (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 these Release Notes

Product Firmware Support
Patch Installation Instructions

These release notes cover ExtremeSecurity for release V7.7.2.6, including patches. These notes cover:

- Firmware support
- Fixes
- Known Issues

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

Product Firmware Support

Status	Firmware Version	Product Type	Release Date
Current Version	7.7.2.6 Build 20160603191354	Customer Software	6/30/2016
Previous Version	7.7.2.6 Build 20160506171537	Customer Software	5/27/2016
Previous Version	7.7.2.6 Build 20160405164932	Customer Software	5/12/2016
Prevous Version	7.7.2.6 Build 20160323173514	Customer Software	04/22/2016
Previous Version	7.7.2.6 Build 20160106113021	Customer Software	02/2/2016
Prevoius Version	7.7.2.6 Build 20151203193508	Customer Software	01/11/2016

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 Networks SIEM Administration Guide*.
- To avoid access errors in your log file, close all open SIEM sessions.
- The fix pack for cannot install 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 725_patchupdate-7.2.5.<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 Review the files in the `/tmp` directory for replication files that might be using up space unnecessarily, such as `tx000XX.sql`.

5 If `tx000xx.sql` files are listed, type the following command to remove these files:

```
rm tx*.sql
```

This prevents a disk space issue from occurring in /tmp that can occur.

6 Create the `/media/updates` directory:

```
mkdir –p /media/updates
```

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

For example: `cd /tmp`

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

```
mount -o loop -t squashfs 725_patchupdate-7.2.5. <build_number>.sfs /
media/updates/
```

9 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.

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

The **all** option updates the software on all systems in your deployment. In HA deployments, primary HA appliances are patched and replicate the patch update to the secondary HA appliance.

If you do not select the **all** option, you copy the fix to each appliance in your deployment and install the fix pack. If you manually install fix packs in your deployment, you must update your appliances in the following order:

1 Console
2 Event Processors
3 Event Collectors
4 Flow Processors
5 Flow Collectors

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.

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

```
umount /media/updates
```

12 Clear the browser cache before logging in to the Console.

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.

2 ExtremeSecurity V7.7.2.5 Patch 6 Release Notes

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.5 Patch 6.

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 7.7.2.5 Build 20151130184502.

Because ExtremeSecurity V7.7.2.5 Patch 6 is a cumulative release, the release notes listed below include fixes assigned to V7.7.2.5 and the issues resolved in V7.7.2.5 Patch 6.

Note
This fix pack can upgrade ExtremeSecurity 7.7.2.4 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 ExtremeSecurity 7.7.2.4 to 7.7.2.5, see the .

Issues Resolved in 7.7.2.5 Patch 6

Product	Number	Description
ExtremeSecurity	IV69698	Accumulator can run out of memory when there are a large number of security profiles and network hierarchy objects.
ExtremeSecurity	IV70750	Message incorrectly states that secondary mh has failed when primary mh's status is unknown in an HA setup.
ExtremeSecurity	IV73207	Globalview configuration persists after globalview is deleted causing unexpected results.
Vulnerability Manager	IV76290	Vulnerability Manager - scan hangs at 1% when scan profile port list exceeds 256 characters.
ExtremeSecurity	IV76403	ExtremeSecurity login attempts can create duplicate user profiles when LDAP group authorization is configured.
ExtremeSecurity	IV77404	'General failure error' when attempting log activity searches.
ExtremeSecurity	IV77833	Patching to ExtremeSecurity 7.2.5.x can fail on some 3128 model appliances.
Vulnerability Manager	IV78699	Time zones that are set within operational windows are disregarded when configured in vulnerability scan.
ExtremeSecurity	IV78839	Toggling on timeseries can appear successful but an error visible in logging can indicate data is not being accumulated.
ExtremeSecurity	IV79271	Patching to ExtremeSecurity 7.2.5 patch 5 causes data and config backups older than 7 days to be deleted.

3 ExtremeSecurity V7.7.2.5 Patch 5 Release Notes

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.5 Patch 5.

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

Important
ExtremeSecurity V7.7.2.5 Patch 5 is no longer available for download, so these release notes are available only as a reference. New features and resolved issues from this patch have been incorporated into Patch 6.

If your deployment is installed with ExtremeSecurity 7.7.2.5, you can install fix pack 7.7.2.5 Build 20151027201330.

Because ExtremeSecurity V7.7.2.5 Patch 5 is a cumulative release, the release notes listed below include fixes assigned to V7.7.2.5 and the issues resolved in V7.7.2.5 Patch 5.

Note
This fix pack can upgrade ExtremeSecurity 7.7.2.4 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 ExtremeSecurity 7.7.2.4 to 7.7.2.5, see the .

Issues Resolved in 7.7.2.5 Patch 5

Product	Number	Description
ExtremeSecurity	IV54720	Managed hosts with an ha secondary might experience a postgres rpm or diskmaint error after a hostservices restart.
ExtremeSecurity	IV67212	Hostcontext service does not automatically restart after daylight savings time change
ExtremeSecurity	IV72003	Configuration backup restores fail on ExtremeSecurity 7.2.4.x installations with 128gb of ram
ExtremeSecurity	IV72734	ExtremeSecurity user interface can become unresponsive in environments with a hundreds of protocol based log sources
ExtremeSecurity	IV73179	Security apar cve-2011-3389: cbc ciphers require modification
FORENSICS	IV73478	ExtremeSecurity incident forensics does not log or audit searches performed by users
ExtremeSecurity	IV73482	Varied process 'out of memory' messages can occur in ExtremeSecurity setups containing many reference sets/maps/tables
ExtremeSecurity	IV73671	Real time streaming of events or flows can intermittently pause for multiple seconds

Product	Number	Description
ExtremeSecurity	IV74082	Restoring a configuration backup that was taken from a ExtremeSecurity nat environment to a non-nat environment fails
ExtremeSecurity	IV74112	Using reference sets as an event filter when creating routing rules is not an available option
ExtremeSecurity	IV74130	Offense reports for generated offenses within a specified time range do not honor the time range
ExtremeSecurity	IV74149	Modifying an scp or sftp log source configured to use an ssh key file can generate an error upon save
ExtremeSecurity	IV74340	The ExtremeSecurity user interface can become unresponsive or unavailable when using the asset_model api
ExtremeSecurity	IV74474	Accumulator 'out of memory' system notifications can occur when using anomaly and behavioral rules
ExtremeSecurity	IV74563	'Top source ip' reports can cause a tx sentry and/or report_runner to run out of memory
ExtremeSecurity	IV74613	An error occurs when attempting to drill down into ExtremeSecurity advanced search results that contain 'assetproperty'
ExtremeSecurity	IV74687	'Include detected events/flows by rule from this point forward...' rule action is not working as expected
ExtremeSecurity	IV74776	Drilling down into the results of a large advanced search query generates a 'bad request...' error message
ExtremeSecurity	IV74997	Improperly formatted advanced search is allowed to run and generates error 'the server encountered an error reading..'
ExtremeSecurity	IV75097	An exception occurs exporting visibile columns from network activity
ExtremeSecurity	IV75830	Frequent tx sentry system notifications related to 'saf_history' can be observed in large ExtremeSecurity deplo
ExtremeSecurity	IV75832	Deploy function for one or more ExtremeSecurity managed hosts can fail
Vulnerability Manager	IV75941	Vulnerability Manager - ExtremeSecurity dashboard rss feeds not working when encryption is enabled on the console and VM processor
ExtremeSecurity	IV75945	Legacy script exists in crontab of high availability secondaries that have been patched up
ExtremeSecurity	IV75993	'Top offenses' report output does not match the corresponding search result output
ExtremeSecurity	IV75998	'An error occurred. An exception has occurred' pop up message navigating the aggregated data management window
Risk Manager	IV76023	Risk Manager - 'an error occurred. An exception has occurred' when selecting configuration monitor on the risks tab
ExtremeSecurity	IV76025	Patching a standalone high availability secondary console to ExtremeSecurity 7.2.5.3 fails during license check
ExtremeSecurity	IV76224	Error 'patch aborted' when patching ExtremeSecurity managed hosts from the console using the patch all option
ExtremeSecurity	IV76232	Rule response limiter is not working when it is limited by anything but the default setting of rule

Product	Number	Description
Vulnerability Manager	IV76405	Vulnerability Manager - 'clean vulnerabilities' action does not work for non-admin ExtremeSecurity users
ExtremeSecurity	IV76603	The '/' partition can exceed disk maintenance thresholds after patching to ExtremeSecurity 7.2.5.x on xx24 and xx28 appliances
ExtremeSecurity	IV76728	Unable to add a log source to 'lack of log source' or 'log source detected' rule test
ExtremeSecurity	IV77107	Expected asset updates might not get applied to the asset model
ExtremeSecurity	IV77141	Unable to add an encrypted managed host to a ExtremeSecurity deployment when port 443 is blocked by firewall rule(s)
FORENSICS	IV77152	Clicking forensics tab gives error '...occurred while parsing the server response:syntax error:unexpected token <'
ExtremeSecurity	IV77440	The 'kipmi0' process can cause 100% cpu usage on some ibm system x series appliances
ExtremeSecurity	IV77603	Users are unable to successfully login to the ExtremeSecurity user interface after correct credentials are entered
ExtremeSecurity	IV77620	Forwarding in json format or forwarding payloads terminated with null characters is not working as intended
ExtremeSecurity	Security Bulletin	Tomcat denial of service
ExtremeSecurity	Security Bulletin	Tomcat security manager bypass
FORENSICS	Security Bulletin	Incident forensics is vulnerable to a sql injection attack
FORENSICS	Security Bulletin	Incident forensics is vulnerable to a cross-site scripting attack
FORENSICS	Security Bulletin	Incident forensics is vulnerable to a session highjack attack
FORENSICS	Security Bulletin	Incident forensics is vulnerable to a man in the middle attack
FORENSICS	Security Bulletin	Incident forensics is vulnerable to a man in the middle attack

4 ExtremeSecurity V7.7.2.5 Patch 4 Release Notes

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.5 Patch 4.

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

If your deployment is installed with ExtremeSecurity 7.7.2.5, you can install fix pack 7.7.2.5 Build 20150831191404.

Because ExtremeSecurity V7.7.2.5 Patch 4 is a cumulative release, the release notes listed below include fixes assigned to V7.7.2.5 and the issues resolved in V7.7.2.5 Patch 4.

Issues Resolved in 7.7.2.5 Patch 4

Product	Number	Description
ExtremeSecurity	IV61456	COLUMN SORTING NOT SORTING INTHE LOG SOURCE WINDOW
ExtremeSecurity	IV64079	VULNERABILITY SCANNER IMPORTS ARE NOT POPULATING ASSET INFORMATION
ExtremeSecurity	IV69873	THE STANDBY HIGH AVAILABILITY 'HA SYSTEM FAILURE' NOTIFICATION MESSAGE ONLY APPEARS WHEN THE STANDBY BOX IS IN 'FAILED' STATE
ExtremeSecurity	IV70662	HA MAY RETAIN OLD CONFIGURATION SETS AND FAIL TO START UP WHEN GOING ACTIVE
ExtremeSecurity	IV70750	MESSAGE INCORRECTLY STATES THAT SECONDARY MH HAS FAILED WHEN PRIMARY MH'S STATUS IS UNKNOWN IN AN HA SETUP
ExtremeSecurity	IV72290	CHECKPOINT LOG SOURCES MIGHT NOT WORK AFTER A FAILOVER TO A HIGH AVAILABILITY SECONDARY
ExtremeSecurity	IV72327	CORE DUMPS CAN OCCUR WHEN A QFLOW APPLIANCE HAS MORE THAN 4 CONFIGURED NETWORK INTERFACES
ExtremeSecurity	IV72625	FLOW FORWARDING FROM 17XX APPLIANCES USING ROUTING RULES DOES NOT WORK
ExtremeSecurity	IV72779	SCHEDULED EEYE SCANNER CONFIGURED USING SNMP V2 DOES NOT RUN
ExtremeSecurity	IV73001	A TX SENTRY CAN OCCUR WHEN ATTEMPTING TO VIEW AN ASSET DETAIL PAGE
ExtremeSecurity	IV73025	A TX SENTRY CAN OCCUR WHEN PERFORMING AN ASSET SEARCH SPECIFYING 'OPERATING SYSTEM CONTAINS'
ExtremeSecurity	IV73090	WINCOLLECT AGENTS CANNOT BE SORTED BY LAST HEART BEAT COLUMN

Product	Number	Description
ExtremeSecurity	IV73120	A REQUIRED CONFIGURATION FILE IS NOT UPDATED WHEN CHANGES ARE MADE TO A FULLY QUALIFIED DOMAIN NAME USING QCHANGE_NETSETUP
ExtremeSecurity	IV73178	'DISK REPLICATION FALLING BEHIND' SYSTEM NOTIFICATIONS ARE GENERATED REPEATEDLY
ExtremeSecurity	IV73219	NO CONTRIBUTING EVENTS ARE DISPLAYED WHEN SELECTING THE 'EVENTS' BUTTON ON AN OFFENSE SUMMARY PAGE
ExtremeSecurity	IV73225	ARIEL SEARCH USING REST API RETURNS ERROR '500' RESPONSE IF A MANAGED HOST IS UNREACHABLE OR AT DIFFERENT VERSION
ExtremeSecurity	IV73400	RULES USING AN ARIEL SEARCH FILTER TEST THAT INCLUDE A REFERENCE SET LOOKUP MIGHT NOT WORK
ExtremeSecurity	IV73451	HIGH AVAILABILITY (HA) SECONDARY CAN REPORT AS BEING IN AN 'UNKNOWN' STATE AFTER PATCHING
ExtremeSecurity	IV73457	A REQUIRED CONFIG ENTRY FOR '/STORE/TRANSIENT/SPILLOVER/QUEUE' MIGHT NOT BE CREATED ON PATCHED MANAGED HOSTS
ExtremeSecurity	IV73484	UNABLE TO ADD SEARCHES USING THE 'INCLUDE IN MY QUICK SEARCHES' OPTION
ExtremeSecurity	IV73599	ExtremeSecurity PATCH INSTALLATION CAN FAIL ON HIGH AVAILABILITY SYSTEMS
ExtremeSecurity	IV73921	DATA NODE BALANCING EXPERIENCES ISSUES OR ERROR MESSAGE 'DATA NODE RE-BALANCING FINSIHED WITH ERROR'
ExtremeSecurity	IV74121	SEARCHES USING A 'GROUP BY' MIGHT CAUSE AN 'APPLICATION ERROR' POP UP
ExtremeSecurity	IV74122	NEWLY INSTALLED WINCOLLECT AGENT MIGHT NOT DISPLAY IN THE WINCOLLECT AGENT LIST
ExtremeSecurity	IV74125	THE MOUSE HOVER OVER POP UP DISPLAYS A BLANK SQUARE ON GROUPED SEARCH RESULTS FOR SOURCE AND DESTINATION IP COLUMNS
ExtremeSecurity	IV74156	APPLYING ExtremeSecurity PATCH TO HIGH AVAILABILITY SECONDARY REPORTS SUCCESSFUL WITH ERRORS
ExtremeSecurity	IV74343	REFERENCE SET PULL DOWNS ARE NOT POPULATED IN LOG ACTIVITY, ADD FILTER, 'REFERENCE SET' DUE TO MISSING USER ROLE PERMISSIONS
ExtremeSecurity	IV74469	USING THE ANOMALY RULE CONDITION 'AND NOT WHEN THE TIME OF DAY IS BETWEEN...' DOES NOT WORK AS EXPECTED
ExtremeSecurity	IV74564	DATA NOTE RE-BALANCING CAN FAIL WITH ERROR 'DATA RE-BALANCING FINISHED WITH ERRORS. I/O ERROR OCCURED WHILE RECEIVING DATA
ExtremeSecurity	IV74989	ExtremeSecurity MANAGED HOSTS ALL DISPLAY THE CONSOLE TIME REGARDLESS OF TIMEZONE SET
ExtremeSecurity	IV75659	INTERMITTENT FAILURE CAN OCCUR WHEN PATCHING UP TO ExtremeSecurity 7.2.5.3
ExtremeSecurity	IV75826	FLOW PROCESSOR CAN INACCURATELY REPORT A LARGE AMOUNT OF SOURCE BYTES AFTER PATCHING

Product	Number	Description
Risk Manager	IV73703	SOME DEVICES MIGHT NOT APPEAR IN THE TOPOLOGY
Risk Manager	IV76177	SUBSEQUENT ExtremeSecurity PATCH 7.2.5.3 ATTEMPT AFTER Risk Manager PATCH 'SRM_UPDATE_117.SQL' IS APPLIED, WILL FAIL THE PATCH TEST
Vulnerability Manager	IV67036	DIFFERENCES IN CRONTAB ENTRIES OF HIGH AVAILABILITY PRIMARY AND SECONDARY
Vulnerability Manager	IV74472	DISCREPANCY IN THE NUMBER OF HOSTS REPORTING VULNERABILITIES WHEN VIEWING SCAN RESULTS

5 ExtremeSecurity V7.7.2.5 Patch 3 Release Notes

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.5 Patch 3.

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

If your deployment is installed with ExtremeSecurity 7.7.2.5, you can install fix pack 7.7.2.5 Build 20150709192800.

Issues Resolved in 7.7.2.5 Patch 3

Product	Number	Description
ExtremeSecurity	IV65976	ERROR GENERATED WHEN ADDING A SEARCH FILTER VALUE WITH A CIDR RANGE ON A CUSTOM PROPERTY CREATED AS 'FIELD TYPE: IP'
ExtremeSecurity	IV66434	ExtremeSecurity UI SYSTEM NOTIFICATION 'PROCESS ECS-EP HAS FAILED TO START' FOR A ExtremeSecurity COLLECTOR
ExtremeSecurity	IV66438	SOME QIDMAP ENTRIES ARE MISSING WHEN USING THE CONTENT MANAGEMENT TOOL TO PERFORM AN EXPORT 'ALL'
ExtremeSecurity	IV68513	RULE NOT FIRING AS EXPECTED DUE TO A REFERENCE SET NAME CONTAINING A CONTROL CHARACTER
ExtremeSecurity	IV69217	SEARCH NAMES CONTAINING UTF MULTIBYTE CHARACTERS DO NOT DISPLAY CORRECTLY AFTER UPGRADE TO ExtremeSecurity 7.2.3
ExtremeSecurity	IV69876'	DAILY START TIME MUST BE BEFORE END TIME' MESSAGE WHEN PROPER CRITERIA IS SET
ExtremeSecurity	IV69893	HOSTCONTEXT OUTOFMEMORY ON DEPLOY IN ENVIRONMENTS THAT HAVE A HIGH NUMBER OF LOG SOURCES
ExtremeSecurity	IV70136	ExtremeSecurity HARDWARE MONITORING SYSTEM NOTIFICATIONS 'RAID CONTROLLER MISCONFIGURATION...'
ExtremeSecurity	IV70510	LOG SOURCES MAY APPEAR WITH INCORRECT STATUS IN LOG SOURCE REPORTING
ExtremeSecurity	IV70528	UNABLE TO IMPORT LARGE REFERENCE SETS OR MAPS
ExtremeSecurity	IV70609	DAILY DATA BACKUPS DO NOT FINISH IN THE ALLOWABLE TIMEFRAME
ExtremeSecurity	IV70642	'IF' INDEX FIELDS SHOULD BE 32-BIT INTEGERS IN QFLOW
ExtremeSecurity	IV70655	ROUTING RULES - NO DROP DOWN LIST IS PRESENTED WHEN SELECTING 'FLOW INTERFACE' FILTER FOR 'FLOWS' DATA SOURCE
ExtremeSecurity	IV70748	SOURCE AND DESTINATION ASSET NAME NOT GETTING POPULATED BY DNS VALUE
ExtremeSecurity	IV70934	CUSTOM QID REFERENCES ON IMPORTED CUSTOM RULES ARE NOT UPDATED

Product	Number	Description
ExtremeSecurity	IV71001	EXPORTING EVENTS FROM LOG OR NETWORK ACTIVITY WITH RESULT LIMITSAPPLIED MAY NOT FUNCTION CORRECTL
ExtremeSecurity	IV71004	HA_SETUP SCRIPT FAILS IN 7.2.4 WHEN ADDRESSESS FOR VIP AND PRI ARE SINGLE OCTET.
ExtremeSecurity	IV71171	REFERENCE SET ELEMENTS OR REFERENCE SET NAMES WITH CERTAIN SPECIAL CHARACTERS IN THEM CANNOT BE DELETED
ExtremeSecurity	IV71359	QFLOW SOURCE AND DESTINATION PORT BASED ANALYSIS IS NOT WORKING AS EXPECTED
ExtremeSecurity	IV71372	NUMERIC VALUE CUSTOM EVENT PROPERTIES PULLED FROM OFFENSE RULES ARE STORED AS INTEGERS WHEN WRITTEN TO REFERENCE SETS
ExtremeSecurity	IV71959	SETTING IPV6 ADDRESSES IN NETWORK HIERARCHY CAUSES FILES TO BE CREATED BY QFLOW0 THAT FILL /STORE/TMP
ExtremeSecurity	IV72303	DASHBOARD WIDGETS NOT DISPLAYING TIMES SERIES DATA FOR NON-ADMIN USERS WITH NON-ADMIN SECURITY PROFILE
ExtremeSecurity	IV72322	THE VULNERABILITY REPORTING AGENT CAN CAUSE DUPLICATE REPORTING OF VULNERABILITY EVENTS
ExtremeSecurity	IV72767	IMPORTING A LARGE QUANTITY OF CHANGES TO THE NETWORK HIERARCHY VIA COMMAND LINE INTERFACE CAUSES DEPLOYS TO TIMEOUT
ExtremeSecurity	IV72840	ExtremeSecurity USER INTERFACE CAN BECOME UNRESPONSIVE IN DEPLOYMENTS WITH A LARGE NUMBER OF MANAGED HOSTS
ExtremeSecurity	IV73033	7.2.4.5 - SAVED SEARCHES THAT HAVE CUSTOM PROPERTIES WITH CAPITAL LETTERS IN THE FILTER ARE NOT WORKING PROPERLY
ExtremeSecurity	IV73064	ExtremeSecurity USER INTERFACE IS INTERMITTENTLY NOT ACCESSIBLE
ExtremeSecurity	IV73087	'FORMATTING ERRORS...' WHEN ATTEMPTING TO REMOVE IP ADDRESS FROM THE SNMP DAEMON SETTINGS IP ACCESS LIST
ExtremeSecurity	IV73351	FILTERS CONTAINING CUSTOM PROPERTIES ARE NOT DISPLAYED IN ROUTING RULES OR EVENT/FLOW RETENTION WINDOWS
ExtremeSecurity	IV73671	REAL TIME STREAMING OF EVENTS OR FLOWS CAN INTERMITTENTLY PAUSE FOR MULTIPLE SECONDS
ExtremeSecurity	IV73698	LOG SOURCE EXTENSIONS NEWLY ASSOCIATED TO LOG SOURCES DO NOT SHOW AS BEING ASSOCIATED IN THE USER INTERFACE
ExtremeSecurity	IV73717	ATTEMPTING TO DELETE A SUBSEQUENT REFERENCE SET IN THE USER INTERFACE WITHOUT REFRESHING THE PAGE FAILS WITH ERROR
ExtremeSecurity	IV73917	DOJO ERRORS OBSERVED IN ExtremeSecurity LOGGING WHEN PERFORMING A ExtremeSecurity USER INTERFACE LOG IN USING THE CHROME WEB BROWSER
ExtremeSecurity	IV74119'	COLLECT LOG FILES' FAILS WITH ERROR 'CAN'T FIND RESULT FILE NAME IN COMMAND OUTPUT'
ExtremeSecurity	IV74681	ExtremeSecurity SYSTEM NOTIFCATIONS 'EVENTS PER INTERVAL THRESHOLD WAS EXCEEDED XX PERCENT OF THE TIME OVER THE PAST HOUR' IN 7.2.5
Risk Manager	IV73352	RISK_MANAGER_BACKUP.LOG FILE GROWS TOO LARGE

Product	Number	Description
Vulnerability Manager	IV70509	INACCURATE VULNERABILITY SCAN TAKES PLACE WHEN "LOW" BANDWIDTH IS SET IN A SCAN PROFILE
Vulnerability Manager	IV71421	USER INTERFACE CAN BECOME UNAVAILABLE WHEN THIRD PARTY VULNERABILITY SCANNER DATA IS IMPORTED INTO ExtremeSecurity
Vulnerability Manager	IV72999	MONTHLY SCHEDULED SCAN DATE CHANGES WHEN THE SCAN PROFILE IS MODIFIED

6 ExtremeSecurity V7.7.2.5 Release Notes

Resolved Issues

Contents

- New features
- Announcement letter
- System requirements
- Installing ExtremeSecurity
- Resolved issues & Known problems

New features

Descriptions of new features are available in the Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.5/com.ibm.qradar.doc_7.2.5/c_qradar_ov_whats_new_722.html).

Announcement letter

The ExtremeSecurity V7.7.2.5 announcement letters are available from IBM's offering page. See the announcements for the following information:

- Detailed product description, including a description of new functions
- Packaging and ordering details

System requirements

For information about hardware and software compatibility, see the detailed system requirements in the .

Installing ExtremeSecurity

For installation instructions, see the .

Resolved Issues

Issues Resolved in 7.7.2.5 Patch 2

Product	Number	Description
ExtremeSecurity	IV73889	OFFENSE GENERATION UNEXPECTEDLY STOPS OCCURRING IN ExtremeSecurity

Issues Resolved in 7.7.2.5 Patch 1

Product	Number	Description
ExtremeSecurity	IV73672	THE ExtremeSecurity USER INTERFACE CAN BECOME INACCESSIBLE DUE TO THE TOMCAT SERVICE RUNNING OUT OF MEMORY

Issues Resolved in 7.7.2.5

Product	Number	Description
ExtremeSecurity	IV42471	WHEN CHANGING GLOBAL CONFIGURATION PASSWORD, IT MAY TAKE A LONG TIME TO COMPLETE.
ExtremeSecurity	IV43440	UNABLE TO FILTER ON CLOSED OFFENSES.
ExtremeSecurity	IV46116	THE HIGH AVAILABILITY (HA) WIZARD FAILS TO ADD A HOST BECAUSE THE IP ADDRESS IS ALREADY DEFINED IN THE SERVER HOST TABLE.
ExtremeSecurity	IV46417	A HARMLESS ERROR MESSAGE MIGHT DISPLAY WHEN YOU APPLY A FIX PACK UPDATE TO YOUR ExtremeSecurity SYSTEM.
ExtremeSecurity	IV50522	EMAIL NOTIFICATIONS FAIL IF THE CONFIGURED EMAIL ADDRESS CONTAINS A HYPHEN "-"
ExtremeSecurity	IV50564	CHANGING FROM THE ALL USER ROLE TO THE ADMIN USER ROLE DOES NOT UPDATE THE EVENT OR FLOW LISTS DISPLAYED ON THE DASHBOARD TABLE.
ExtremeSecurity	IV50732	LIST OF EVENTS DOES NOT DISPLAY PROPERLY DUE TO HTML PARSING ERROR WHEN YOU USE THE MICROSOFT INTERNET EXPLORER 8 WEB BROWSER.
ExtremeSecurity	IV50740	PENDING AUTOMATIC UPDATES MIGHT INSTALL UNEXPECTEDLY WHEN YOU UPDATE A SCHEDULE ON THE UPDATES WINDOW.
ExtremeSecurity	IV51020	UNABLE TO CREATE A LOG SOURCE ONLY OR NETWORK ONLY SECURITY PROFILE WITHOUT BOTH LOG SOURCES AND NETWORKS SPECIFIED
ExtremeSecurity	IV54327	SOURCE AND DESTINATION ASSET NAME COLUMNS DO NOT QUERY THE HOSTNAME COMPONENT OF THE ASSET PROFILE.
ExtremeSecurity	IV54471	MODIFYING A REPORT TEMPLATE MIGHT NOT ALLOW USERS TO CHANGE THE END DATE OF THE REPORT BEYOND SEPTEMBER 16, 2010.
ExtremeSecurity	IV54685	NETWORK I/O ISSUES ON A MANAGED HOST MIGHT GENERATE AN OUT-OF-MEMORY ISSUE ON THE CONSOLE.
ExtremeSecurity	IV54705	ARIELCLIENT CONTAINS ADDITIONAL LINE FEED AT THE END OF FILE.
ExtremeSecurity	IV55696	CANNED QUICK SEARCHES DO NOT SHOW IN MANAGE SEARCH RESULTS BUT CUSTOM QUICK SEARCHES DO.
ExtremeSecurity	IV56033	PERFORMING A SORT OF SEARCH RESULTS FOR AN IN-PROGRESS SEARCH GIVES ERROR 'THIS QUERY HAS TIMED OUT AND IS NO LONGER VALID.
ExtremeSecurity	IV56451	BULK ADD OF LOG SOURCES MAY GENERATE AN F5 ERROR ON THE UI.
ExtremeSecurity	IV57325	DATA ACCUMULATION AND UNIQUE COUNT MAY NOT BE DISPLAYED FOR THE ADMIN ON SEARCHES CREATED BY NON-ADMIN USERS.

Product	Number	Description
ExtremeSecurity	IV58681	FILTERING ON A CUSTOM PROPERTY THAT CONTAINS THE SUBSTRING "ID:"RETURNS NO RESULTS.
ExtremeSecurity	IV59099	INCORRECT HOST.TOKEN CAUSES EXTERNAL AUTHENTICATION TO FIRE FOR "SEC" USER.
ExtremeSecurity	IV59873	ADDING CUSTOM EVENT PROPERTIES WITH CERTAIN SPECIAL CHARACTERS CAN CAUSE AN EXCEPTION WHEN FILTERING.
ExtremeSecurity	IV59990	LOG ACTIVITY SEARCH SHOWS WRONG DATE WHEN THE DASHBOARD GRAPHS HAVEN'T FULLY LOADED AND VIEW IS PRESSED IN LOG ACTIVITY.
ExtremeSecurity	IV60091	DHCPV6 FLOW TRAFFIC BEING PARSED WITH INCORRECT EVENT NAME AND LOW LEVEL CATEGORY.
ExtremeSecurity	IV60208	AFTER AN UPGRADE TO ExtremeSecurity 7.2.2 PATCH 1, NEW LOG SOURCES DO NOT AUTOMATICALLY DISCOVER ON MANAGED HOSTS
ExtremeSecurity	IV60574	ARIEL RIGHT CLICK API DOES NOT WORK ON ARIEL PROPERTIES.
ExtremeSecurity	IV61205	APPLICATION ERROR IN MANY PAGES FOR USER WITH $ IN USERNAME.
ExtremeSecurity	IV61910	SEARCHES THAT COMBINE HIGH AND LOW CATEGORY SEARCH VALUE FILTERS RETURN INCORRECT RESULTS..
ExtremeSecurity	IV62434	X-FORCE RULES TRIGGER EVEN WHEN TARGETING TRUSTED (NON-MALICIOUS) DOMAINS
ExtremeSecurity	IV62512	UNABLE TO CHANGE LANGUAGE SETTINGS AS NON-ADMINISTRATOR USER.
ExtremeSecurity	IV63067	1705 APPLIANCES SHOW UP AS 1701 APPLIANCES IN THE SYSTEM AND LICENSE MANAGEMENT SCREEN OF THE UI.
ExtremeSecurity	IV63125	ADDING A SECONDARY TO A MANAGED HOST MAY FAIL DUE TO /STORE BEING BUSY ON THE SECONDARY.
ExtremeSecurity	IV63420	ASSETPROFILER ERRORS IN ExtremeSecurity.LOG THAT REFER TO MESSAGEMARSHALLERV2
ExtremeSecurity	IV63466	THE 'EVENT PROCESSOR' SEARCH FILTER DOES NOT WORK WHEN SETUP IN RULES.
ExtremeSecurity	IV63939	SEARCHES AND/OR REPORTS THAT CONTAIN THE COLUMN 'SOURCE ASSET NAME' AND ARE GROUPED BY SOURCE IP WILL RETURN 'NONE'.
ExtremeSecurity	IV64549	IPFIX AND NETFLOW V9 ONLY READS 16-BIT AND NOT 32-BIT ASN NUMBERS.
ExtremeSecurity	IV64741	ExtremeSecurity SOFTWARE ONLY INSTALLATION ON CUSTOMER SUPPLIED HARDWARE WITH XX28 SPECIFICATIONS MAY FAIL DURING SETUP.
ExtremeSecurity	IV64777	REPORTS RETURN DIFFERENT DATA WHEN RUN AGAINST RAW DATA VERSUS A SCHEDULED/ACCUMULATED DATA REPORT.
ExtremeSecurity	IV65085	WHEN LOGGING INTO THE ExtremeSecurity USER INTERFACE, CERTAIN DASHBOARD ITEMS SHOW AN ERROR MESSAGE.
ExtremeSecurity	IV65502	RULES THAT USE 'INCLUDE DETECTED EVENT FROM THIS ATTACKER FROM THIS POINT FORWARD' ARE NOT ADDING NEW EVENTS TO THE OFFENSE.

Product	Number	Description
ExtremeSecurity	IV65584	WHEN APPLYING A LOG SOURCE EXTENSION TO A LOG SOURCE TYPE, THE USER INTERFACE APPEARS TO NOT APPLY THE CHANGE SUCCESSFULLY.
ExtremeSecurity	IV65935	OFFENSE SEARCH 'SAVE CRITERIA' OPTION THAT CONTAINS A 'SOURCE NETWORK' FUNCTIONS CORRECTLY BUT DOES NOT DISPLAY PROPERLY.
ExtremeSecurity	IV66213	NEWLY CREATED ExtremeSecurity DASHBOARDS ARE ACCESSIBLE TO ALL USERS WITH THE SAME ASSIGNED USER ROLE.
ExtremeSecurity	IV66756	UNABLE TO LOAD THE 'LOG SOURCES' PAGE IN THE ExtremeSecurity UI AFTER PATCHING FROM 7.1.2.X TO 7.2.X.
ExtremeSecurity	IV67083	RULES ARE NO LONGER ASSOCIATED TO OFFENSES AFTER A SOFT CLEAN SIM IS PERFORMED.
ExtremeSecurity	IV67212	HOSTCONTEXT SERVICE DOES NOT AUTOMATICALLY RESTART AFTER DAYLIGHT SAVINGS TIME CHANGE.
ExtremeSecurity	IV67219	EMPTY PLUG-INS OPTION ON ADMIN TAB IN THE ExtremeSecurity USER INTERFACE.
ExtremeSecurity	IV67325	SNMP DAEMON IS NOT ENABLED ON HIGH AVAILABILITY SECONDARY.
ExtremeSecurity	IV67522	THE REMOVE ITEM OPTION FROM WITHIN A TIME SERIES GRAPH DOES NOT ALWAYS WORK AS EXPECTED IN CHROME WEB BROWSER.
ExtremeSecurity	IV67755	ExtremeSecurity DATA BACKUPS MIGHT FAIL TO RUN SUCCESSFULLY ON MANAGED HOSTS.
ExtremeSecurity	IV67807	THE ARIEL RIGHTCLICK.PROPERTIES API DROPS THE '\' OR '$' CHARACTERS IN EVENT PROPERTIES.
ExtremeSecurity	IV67847	FILTERED NETWORK ACTIVITY SEARCHES MAY RETURN UNEXPECTED RESULTS.
ExtremeSecurity	IV67939	SILENT INSTALLS DO NOT WORK IN 7.2.4.
ExtremeSecurity	IV68011	AN 'APPLICATION ERROR' POP UP WINDOW OCCURS WHEN CREATING A FLOW RULE THAT TESTS AGAINST REFERENCE TABLE DATA.
ExtremeSecurity	IV68343	APPLYING ExtremeSecurity PATCH .SFS FAILS ON HIGH AVAILABILITY SECONDARY.
ExtremeSecurity	IV68596	'AN ERROR HAS OCCURRED. REFRESH YOUR BROWSER...' MESSAGE WHEN ATTEMPTING TO DISABLE OR DELETE A RULE IN ExtremeSecurity.
ExtremeSecurity	IV68877	TIME ZONE DATA DISPLAYED WITHIN ExtremeSecurity IS NOT ACCURATE FOR SOME TIME ZONES.
ExtremeSecurity	IV69168	SAVED SEARCHES WITH SPECIAL CHARACTERS CAUSES DASHBOARDS TO DISAPPEAR.
ExtremeSecurity	IV69695	WHEN DASHBOARDS ARE ADDED TO USER ROLES, THOSE USERS WILL NO LONGER SEE THE DEFAULT DASHBOARDS.
ExtremeSecurity	IV69750	IDENTITY HOSTNAME IS BEING POPULATED BY USERNAME IN OFFENSE.
ExtremeSecurity	IV69817	QFLOW CRASHES IF PACKET SOURCE ADAPTOR IS DISABLED.
ExtremeSecurity	IV69895	UNABLE TO RESTORE CONFIG BACKUP FOR NON-ENGLISH UI.
ExtremeSecurity	IV70515	EVENTPROCESSOR FILTER IN ADVANCED QUERY AND RESTAPI QUERIES ALL EVENT PROCESSORS WHEN SPECIFYING A SPECIFIC EVENT PROCESSOR.

Product	Number	Description
ExtremeSecurity	IV70522	'ERROR: NULL VALUE IN COLUMN' WHEN ADDING A NEW ADMIN USER ACCOUNT WITH EXTERNAL AUTH AND NO PASSWORD IS ENTERED.
ExtremeSecurity	IV70525	RESPONSE TIME WHEN CONFIGURING A LOG SOURCE IS VERY SLOW WHEN USING WITH CHROME.
ExtremeSecurity	IV70601	ARIEL ERROR WHEN FILTERING ON A SORTED, AGGREGATED COLUMN.
ExtremeSecurity	IV71009	DELETING REFERENCE SETS USED IN RULES FAILS, BUT DOESN'T WARN WHY.
ExtremeSecurity	IV71013	RE-EDITING REPORT DESCRIPTION SHOWS HTML </BR>.
ExtremeSecurity	IV71265	DASHBOARD LEGENDS BLEEDING HTML CODE IN TOOLTIP.
ExtremeSecurity	IV71266	DSM JAR FILES ARE NOT BEING PROPERLY RESTORED FROM A CONFIG BACKUP.
ExtremeSecurity	IV71980	'DOMAIN' DOES NOT WORK AS A SEARCH FILTER WHEN USING THE ExtremeSecurity ADVANCED SEARCH FUNCTIONS.
ExtremeSecurity	IV72129	'AN INVALID CURSOR WAS PROVIDED TO THE QUERY. PLEASE TRY AGAIN' WHEN A LOG OR NETWORK ACTIVITY SEARCH IS PERFORMED.
ExtremeSecurity	IV72736	RESTAPI EVENTS ARE DISPLAYING AS 'UNKNOWN' EVENTS.
ExtremeSecurity	IV72903	SYSTEM NOTIFICATION ERROR 'OUT OF MEMORY DISCOVERED FOR HOSTCONTEXT' DURING BACKUP PROCESS.
ExtremeSecurity	IV72934	NULLPOINTEREXCEPTION IN ExtremeSecurity LOG FILES CAUSED BY AN INVALID REGULAR EXPRESSION (REGEX) IN A RULE SEARCH FILTER TEST.
ExtremeSecurity	IV73043	THE /STORE/TRANSIENT PARTITION DOES NOT GET RE-MOUNTED AFTER PERFORMING A FACTORY RE-INSTALL USING THE 7.2.4 ISO.
Risk Manager	IV69656	Risk Manager MULTILINE LOG MESSAGE PRODUCES EXCESSIVE EVENTS IN ExtremeSecurity.
Vulnerability Manager	IV73452	SCHEDULED SCANS DO NOT APPEAR IN THE SCHEDULED SCANS CALENDAR.
Vulnerability Manager	IV70824	AUTOMATIC POST SCAN REPORTS ARE NOT BEING GENERATED.
Vulnerability Manager	IV67786	ERROR MESSAGE RETURNED WHEN ATTEMPTING TO UPLOAD A VM LICENSE.

Known problems

There are no known issues to report at this time.