Extreme Networks Security Analytics Release Notes

For Software Version 7.7.2.6

9034922-06

Published June 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: www.extremenetworks.com/documentation/

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

- *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.

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 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 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 726_patchupdate-7.2.6. <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.

After all hosts are updated, administrators can send an email to their team to alert them that browser caches must be cleared before logging in to the SIEM interface.

2 Release Notes for Extreme Security V7.7.2.6 Patch 6

Extreme Networks is pleased to introduce the Extreme Security V7.7.2.6 Patch 6.

If your deployment is installed with Extreme Security 7.7.2.4 or later, you can install fix pack 7.7.2.6 Build 20160603191354.

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

Note
The `7.2.6-QRADAR-QRSIEM-20160506171537` fix pack can upgrade Extreme Security 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 Extreme Security 7.2.4 to Extreme Security 7.7.2.6, see the *Extreme Networks Security Upgrade Guide*.

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	IV79651	NEWLY ADDED DATA NODE DISPLAYS A STATUS OF 'WAITING' AND DOES NOT PROGRESS
EXTREME SECURITY	IV79846	SOME OFFENSE REPORTS CAN BE EMPTY WHEN MULTIPLE DOMAINS ARE PRESENT IN DOMAIN MANAGEMENT
EXTREME SECURITY	IV82557	`ERROR OCCURED WHILE SEARCHING FOR DEPENDENTS` MESSAGE WHEN ATTEMPTING TO DELETE A RULE FROM THE USER INTERFACE
EXTREME SECURITY	IV83323	'SOURCEFIRE 3D' DEVICE BACKUP RESULTS IN PARSE WARNING
EXTREME SECURITY	IV83535	REPORT ON TOP OFFENSES THAT ARE BASED ON SAVED SEARCHES CONTAINING DOMAIN FILTERS DO NOT WORK AS EXPECTED
EXTREME SECURITY	IV84689	OFFLINE FORWARDING FROM DATA NODES DOES NOT WORK

3 Release Notes for Extreme Security V7.7.2.6 Patch 5

Extreme Networks is pleased to introduce the Extreme Security V7.7.2.6 Patch 5.

If your deployment is installed with Extreme Security 7.7.2.4 or later, you can install fix pack 7.7.2.6 Build 20160506171537.

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

Note
The `7.2.6-QRADAR-QRSIEM-20160506171537` fix pack can upgrade Extreme Security 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 Extreme Security 7.2.4 to Extreme Security 7.7.2.6, see the *Extreme Networks Security Upgrade Guide*.

Resolved Issues

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

EXTREME SECURITY	IV75011	QCHANGE_NETSETUP DOES NOT DISPLAY CURRENT EMAIL SERVER THAT HAS PREVIOUSLY BEEN CONFIGURED
EXTREME SECURITY VULNERABILITY MANAGER	IV75919	ERROR MESSAGE POP UP WHEN SAVING A SCAN PROFILE THAT REFERENCES A SCAN POLICY CONTAINING DOUBLE QUOTATION MARKS
EXTREME SECURITY VULNERABILITY MANAGER	IV76237	THE USER INTERFACE CAN BECOME INACCESSIBLE DUE TO A JAVA.LANG.EXCEPTION
EXTREME SECURITY	IV76497	'RAID CONTROLLER MISCONFIGURATION...' SYSTEM NOTIFICATIONS GENERATED FOR HIGH AVAILABILITY SECONDARY APPLIANCES
EXTREME SECURITY	IV77148	CHANGES MADE AND SAVED TO A LARGE NETWORK HIERARCHY CAN APPEAR TO HANG AND NEVER COMPLETE
EXTREME SECURITY	IV77154	SOME FIELDS ARE NOT POPULATED WITH CORRECT DATA IN SNMP TRAP GENERATED RESPONSES TO A FIRED OFFENSE RULE
EXTREME SECURITY	IV77888	EXCESSIVE HOSTCONTEXT STARTUP AND SHUTDOWN TIMES ON EXTREME SECURITY CONSOLES AT VERSION 7.2.5.X CAN SOMETIMES BE EXPERIENCED
EXTREME SECURITY VULNERABILITY MANAGER	IV77930	UNABLE TO HAVE A VULNERABILITY MANAGER SCANNER RUNNING ON A CONSOLE WHILE ALSO HAVING AN ENCRYPTED VULNERABILITY MANAGER APPLIANCE

EXTREME SECURITY	IV78823	INACCURATE MESSAGE 'WAITING FOR DATA RE-BALANCING' CAN DISPLAYED FOR AN EVENT PROCESSOR-DATA NODE SETUP
EXTREME SECURITY	IV79254	THE EXTREME SECURITY USER INTERFACE CAN SOMETIMES RESTART ITSELF UNEXPECTEDLY ON DEPLOYMENTS USING X-FORCE
EXTREME SECURITY	IV79698	NON-ADMIN USERS ASSIGNED TO A DOMAIN ARE UNABLE TO SWITCH REPORT GROUPS
EXTREME SECURITY VULNERABILITY MANAGER	IV79931	VULNERABILITY MANAGER SCAN PROFILE SCREEN CAN DISPLAY INCORRECT DATE/TIME VALUES FOR THE 'END OF LAST RUN'
EXTREME SECURITY	IV80154	REPORTS WITH MISSING TEMPLATE XML'S CANNOT BE DELETED FROM THE USER INTERFACE REPORTS TAB
EXTREME SECURITY	IV80635	UNABLE TO LOG IN TO EXTREME SECURITY CONSOLE FROM ANY COMPUTER ON A 172.17.0.0/16 IP RANGE
EXTREME SECURITY	IV80669	PARSING FOR LOG SOURCE EXTENSION (LSX) RELATED EVENTS CAN SOMETIMES FAIL TO OCCUR ON APPLIANCES UNDER A HEAVY LOAD
EXTREME SECURITY	IV80835	ADVANCED SEARCH FUNCTION 'LONG' DOES NOT WORK IN COMBINATION WITH SOME OTHER FUNCTIONS
EXTREME SECURITY	IV80837	MANAGED HOST DATA BACKUPS CAN SOMETIMES FAIL AFTER PATCHING TO EXTREME SECURITY 7.2.6.X
EXTREME SECURITY	IV81173	RULE RESPONSE 'OFFENSE NAMING' DOES NOT ALWAYS WORK AS EXPECTED
EXTREME SECURITY	IV81311	'CANNOT RETRIEVE THE SECURITY DATA DISTRIBUTION INFORMATION' ERROR WHEN NAVIGATING SYSTEM AND LICENSE MANAGEMENT
EXTREME SECURITY	IV81396	A CONTENT MANAGEMENT TOOL IMPORT CAN FAIL TO SUCCESSFULLY IMPORT SOME CONFIGURED LOG SOURCES
EXTREME SECURITY	IV81461	LARGE NUMBER OF SIEM-AUDIT-2 SYSTEM GENERATED EVENTS WITHIN EXTREME SECURITY
EXTREME SECURITY	IV81669	ERRORS IN EXTREME SECURITY LOGGING: 'SCANNER NAME (ID #)' WAS FOUND IN THE DATABASE, BUT IS FLAGGED AS DELETED, NOT INITIALIZING
EXTREME SECURITY	IV81675	EXTREME SECURITY USER INTERFACE CAN BECOME UNAVAILABLE DUE TO TOMCAT TXSENTRY DURING CERTAIN ASSET API CALLS
EXTREME SECURITY VULNERABILITY MANAGER	IV82472	VULNERABILITY MANAGER SCANS MAY NEVER COMPLETE WHEN TOOLS FAIL TO PARSE BINARY DATA
EXTREME SECURITY	IV82541	UNABLE TO DELETE SAVED SEARCHES AND RULES FROM THE EXTREME SECURITY USER INTERFACE
EXTREME SECURITY	IV82558	ATTEMPTING TO ADD AN ADDITIONAL FLOW FORWARDING DESTINATION DOES NOT WORK
EXTREME SECURITY	IV82734	ADDITIONAL INTERFACES CONFIGURED ON HIGH AVAILABILITY (HA) APPLIANCES MIGHT NOT START UP CORRECTLY AFTER A REBOOT
EXTREME SECURITY	IV82767	THE PROCESS OF ADDING A NEW OR REBUILT HIGH AVAILABILITY (HA) SECONDARY CAN FAIL IN SOME CIRCUMSTANCES
EXTREME SECURITY VULNERABILITY MANAGER	IV82768	ERROR MESSAGE `ILLEGAL HEX CHARACTERS IN ESCAPE` WHEN ENTERING A PASSWORD CONTAINING SPECIAL CHARACTERS

EXTREME SECURITY	IV82817	NETWORK HIERARCHY ENTRIES CONTAINING LANGUAGE CHARACTERS OTHER THAN ENGLISH CAN BE REMOVED DURING A PATCH
EXTREME SECURITY	IV82933	CHANGES MADE TO REMOTE NETWORKS ARE NOT PRESERVED OR IMPLEMENTED
EXTREME SECURITY	IV83022	REQUIRED EXTREME SECURITY APPLIANCE SERVICE DOES NOT SUCCESSFULLY RESTART AFTER AN OUT OF MEMORY OCCURRENCE
EXTREME SECURITY VULNERABILITY MANAGER	IV83088	VULNERABILITY MANAGER SCANS THAT CONTAIN " -- " (DOUBLE HYPHEN) IN THE SCAN PROFILE NAME RESULT IN APPLICATION ERROR
EXTREME SECURITY	IV83191	X-FORCE UPDATES CAN FAIL AFTER PATCHING EXTREME SECURITY TO 7.7.2.5 PATCH 5
EXTREME SECURITY VULNERABILITY MANAGER	IV83194	VULNERABILITY MANAGER RISK MANAGER REPORT THAT INCLUDES 'DEVICE RULES' CAN FAIL AFTER PATCHING EXTREME SECURITY
EXTREME SECURITY	IV83422	HIGH AVAILABILITY SECONDARY IN A FAILED STATE AFTER PERFORMING AN HA ADD OR HA RESTORE FUNCTION, NO SSH CONNECTIVITY
EXTREME SECURITY	IV83461	LDAP GROUP AUTHENTICATION CAN SOMETIMES FAIL IF THE USER CN CONTAINS A COMMA
EXTREME SECURITY	IV83463	JSON EVENT FORWARDING VIA A RULE RESPONSE DOES NOT INCLUDE THE ASSOCIATED RULE NAME IF THE OPTION IS SELECTED
Extreme Networks Security Incident Forensics	IV83464	RECOVERIES COMPLETE SUCCESSFULLY BUT NO DOCUMENTS ARE GENERATED WHEN THERE IS VLAN TRAFFIC WITHIN A VLAN
EXTREME SECURITY	IV84009	UNABLE TO EDIT REFERENCE SET 'TIME TO LIVE ELEMENTS' FROM THE EXTREME SECURITY USER INTERFACE

4 Release Notes for Extreme Security V7.7.2.6 Patch 4

Extreme Networks is pleased to introduce the Extreme Security V7.7.2.6 Patch 4.

If your deployment is installed with Extreme Security 7.7.2.4 or later, you can install fix pack 7.7.2.6 Build 20160405164932.

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

Note
The `7.2.6-QRADAR-QRSIEM-20160405164932` fix pack can upgrade Extreme Security 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 Extreme Security 7.2.4 to Extreme Security 7.7.2.6, see the *Extreme Networks Security Upgrade Guide*.

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	IV83336	Adding a flow collector can fail and replication to flow collectors can fail due to an Extreme Security replication issue.
Extreme Security	IV83506	Apps (extension management) can no longer be installed after patching to Extreme Security 7.7.2.6 Patch 3.

5 Release Notes for Extreme Security V7.7.2.6 Patch 3

Extreme Networks is pleased to introduce the Extreme Security V7.7.2.6 Patch 3.

If your deployment is installed with Extreme Security 7.7.2.4 or later, you can install fix pack 7.7.2.6 Build 20160323173514.

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

Note
The `7.2.6-QRADAR-QRSIEM-20160323173514` fix pack can upgrade Extreme Security 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 Extreme Security 7.2.4 to Extreme Security 7.7.2.6, see the *Extreme Networks Security Upgrade Guide*.

Important
An issue with QFlow Collector (12xx &13xx) appliances and replication has been discovered in Extreme Security 7.7.2.6 Patch 3. Administrators with QFlow Collectors should not install this patch until APAR IV83336 is resolved. It might take up to 12 hours for the APAR to be visible online.

Installation Notes

Ensure that you take the following precautions:

- If you have QFlow Collectors (12xx / 13xx) appliances in your deployment, you should not install this Fix Pack due to a replication issue as mentioned above. For more information, see https://www.ibm.com/support/entdocview.wss?uid=swg1IV83336.
- For the installation procedure, see Patch Installation Instructions on page 6.

Resolved Issues

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

Issues resolved in 7.2.6 Patch 3		
Product	Number	Description
N/a	Security Bulletin	Multiple vulnerabilities in openssl affect Extreme SIEM and Extreme Security Incident Forensics.
Extreme Security	IV50569	Email rule response specifies the wrong source IP address when a superflow triggered the rule.

Issues resolved in 7.2.6 Patch 3		
Extreme Security	IV54648	The bb:categorydefinition: firewall or acl accept incorrectly matches websense "access permitted" event categories.
Extreme Security	IV62092	Searches using "payload matches regular expression" do not work when using range quantifiers.
Extreme Security	IV63146	Graphing of last data point in the ui are inaccurately displayed.
Extreme Security	IV64622	Unable to delete a custom property that is associated with a saved search.
Extreme Security	IV65968	The 'system time' displayed when using the asia/jerusalem timezone setting is different than the command line time.
Extreme Security	IV66639	When setting up routing rules using 'log source group', those events do not get forwarded.
Extreme Security	IV67203	Filtering by country/geographic region may return inconsistent results.
Extreme Security	IV67458	Rules that compare a numerically formatted custom property to a numerical reference set fail to match.
Extreme Security	IV67506	ISO27001 reports rely on a rule that is no longer within Extreme Security.
Extreme Security	IV67808	Source or destination IP list for superlfows is truncated.
Extreme Security	IV69110	Asset profiler does not fully remove assets, leaving 'empty' assets.
Extreme Security	IV69896	Asset details additional page viewing not working.
Extreme Security	IV70136	Extreme Security hardware monitoring system notifications 'raid controller misconfiguration.
Extreme Security	IV70523	Using multiple 'group by' will cause global view to be incorrect when trying to accumulate data.
Extreme Security	IV70530	User able to view log source groups outside of security profile rule.
Extreme Security	IV70750	Message incorrectly states that secondary mh has failed when primary mh's status is unknown in an ha setup.
Extreme Security	IV70752	Reload of saved search with depracated settings and deleting regex custom property will both fail.
Extreme Security	IV70961	Destination IP is being marked as 127.0.0.1 when no IP is specified in Extreme Security's traffic.
Extreme Security	IV71073	Dashboard items with a specific interval saved in the criteria do not function correctly.
Extreme Security Vulnerability Manager	IV71421	Vulnerability Manager - user interface can become unavailable when third party vulnerability scanner data is imported into Extreme Security.
Extreme Security	IV72992	Extreme Security network hierarchy does not display more than the first 100 top level groups.
Extreme Security	IV73700	Large quantity of Extreme Security API audit logs.

Issues resolved in 7.2.6 Patch 3		
Extreme Security	IV74089	Some geodata displayed within Extreme Security detailing IP country of origin is not correct.
Extreme Security	IV74113	Source and destination IP display as 'unauthorized' in the offense list.
Extreme Security	IV74153	Custom rule engine log sources show as 'error' in log source reporting.
Extreme Security	IV74396	New or edited wincollect log sources target 'external' destination displays the target 'internal' destination.
Extreme Security	IV74566	'Performance degradation' and/or 'dropped events' system messages when syslog events contain chained hostnames.
Extreme Security	IV74690	Expired license warnings related to high availability secondary appliances that have been removed from a deployment.
Extreme Security	IV74693	Log source extensions might fail to parse events as expected when more than nine capture groups exist.
Extreme Security Vulnerability Manager	IV74850	Vulnerability Manager - scan summary report displays information from previously scanned target.
Extreme Security	IV75854	Error message 'there was a problem connecting to the query server. Please try again later' after performing a deploy.
Extreme Security	IV75864	The LADP authentication configuration user interface page can timeout when attempting to save a configuration.
Extreme Security	IV75994	A nullpointerexception can occur during heavy offense update traffic causing offenses to stop generating.
Extreme Security	IV76356	X-force rules can fire unexpectedly in Extreme Security environments with encryption enabled.
Extreme Security	IV76601	Unable to apply license to an event processor high availability cluster that is in a log manager console deployment.
Extreme Security	IV76671	Selecting a dashboard item setting button (gear) can cause the dashboard item to disappear when using internet explorer.
Extreme Security	IV76722	Shared dashboard items do not always retain all the dashboard item settings.
Extreme Security	IV76724	Response limiter displays non-applicable options for rules using the 'lack of device' test.
Extreme Security	IV76855	Extreme Security deployments with hundreds of thousands of log sources cansee pipeline processing performance degradation.
Extreme Security	IV77041	Hostcontext 'out of memory' can occur on managed hosts during a deploy function.
Extreme Security	IV77044	Event/flow parsing can stop and events/flows dropped messages can be caused by a process deadlock.

Issues resolved in 7.2.6 Patch 3		
Extreme Security	IV77069	'Operating system' is not included in an asset export.
Extreme Security	IV77110	'Warn' message visible in Extreme Security logging '[warn]...cannot retrieve jmx port number for process: pair (scaserver,null).
Extreme Security	IV77410	Searches containing an event processor filter give error 'event processor is unknown host' after patching to Extreme Security 7.7.2.5.
Extreme Security	IV77428	The 'save results' option from within 'edit search' and 'new search' does not protect the search results.
Extreme Security	IV77435	Referencedatautil.sh does not return expected results
Extreme Security	IV77437	Default dashboard item settings are inconsistent for new Extreme Security users with the same security roles.
Extreme Security	IV77438	/var/log/ partition on high availability secondaries can run out of free space due to the '/var/log/systemstabmon/' folder.
Extreme Security	IV77612	The default API cursor retention setting of five days can sometimes cause '/store/transient' to run out of free space.
Extreme Security	IV77643	Extreme Security log manager user dashboard item changes are not preserved on subsequent logins.
Extreme Security	IV77645	Modifying a reference set blacklist rule causes associated rules to not load. Error message: 'failed to load data!'.
Extreme Security	IV77669	Extreme Security 'ldap' authentication: unable to add multiple users from different groups from the ldap root directory.
Extreme Security	IV77671	Offenses can stop being generated in Extreme Security.
Extreme Security Risk Manager	IV77673	Risk Manager can generate an excessive amount of warning messages being logged.
Extreme Security	IV77721	Time synchronization issues between the console and managed hosts.
Extreme Security	IV77767	Extreme Security user interface outages can occur when trying to load the managed search results page.
Extreme Security	IV77861	Authorized services API can sometimes fail with a nullpointerexception written to logs.
Extreme Security	IV77864	Generic error returned when trying to add cidr ranges to a reference set.
Extreme Security	IV77880	Custom rule dependencies are sometimes not observed when using a search filter rule test.
Extreme Security	IV77935	Extreme Security advanced searches containing 'assetproperty' can sometimes fail with no errors displayed in the user interface.
Extreme Security	IV77936	An asset can show up in the incorrect network hierarchy after its IP address is manually changed.

Issues resolved in 7.2.6 Patch 3		
Extreme Security	IV77937	Offenses can fail to be generated when network names in network hierarchy end with a period or dot.
Extreme Security	IV78165	Null field data in reference sets entered using the Extreme Security user interface can cause nullpointerexceptions.
Extreme Security	IV78271	Creating a new vulnerability scanner and then initiating an initial scan can fail on first attempt.
Extreme Security	IV78272	Bulk added log source groups that are deleted using the user interface still remain in the Extreme Security database.
Extreme Security	IV78275	Attempting to navigate within an offense to related offenses can sometimes yield incorrect results.
Extreme Security	IV78305	Using the enter key within 'close offense note:' field can result in being redirected instead of moving to the next line.
Extreme Security	IV78319	'Error generating sql chart' message instead of the expected chart in a generated report.
Extreme Security	IV78322	Offense searches can sometimes generate an 'application error' pop up.
Extreme Security	IV78345	Event processing on event processors might stop when the number of event collectors exceeds the pool size.
Extreme Security	IV78458	Some custom event properties used to populate reference tables can be removed from rule responses after patching Extreme Security.
Extreme Security	IV78469	The Extreme Security default flow rules that are used to detect ssh or telnet traffic on a non-standard port sometimes do not fire.
Extreme Security	IV78521	Some rule tests can generate benign nullpointerexception messages on non-consoles.
Extreme Security Vulnerability Manager	IV78522	Paging functions on the Vulnerability Manager 'scan exclusions' page does not work as expected.
Extreme Security	IV78544	High availability crossover routing does not work when using non default IP addressing.
Extreme Security	IV78563	Offense reports can sometimes display incorrect offense username data.
Extreme Security	IV78566	Using advanced searches that contain 'assethostname' functions can sometimes fail.
Extreme Security	IV78705	Offense name sometimes does not match the naming specifications of the contributing rules.
Extreme Security	IV78800	Extreme Security REST API can sometimes return no search results.
Extreme Security vuln. Manager	IV78809	System notification 'a scan tool has stopped unexpectedly, in some cases this may cause the scan to be stopped'.

Issues resolved in 7.2.6 Patch 3		
Extreme Security	IV78824	A data node can experience an ariel_query_server out of memory after event/flow processor communication loss.
Extreme Security	IV78841	Pipeline processing issues can sometimes occur in Extreme Security deployments causing dropped and/or stored events.
Extreme Security	IV78844	Xforce url rules can sometimes cause events being routed directly to storage messages.
Extreme Security	IV78853	Multiple 'default_netflowoffset length past end of buffer at offest' messages in qflow logging.
Extreme Security	IV79068	Time zone data for turkey and moscow can be incorrect due to changes in Daylight Savings Time (DST).
Extreme Security	IV79077	High availability (ha) wizard can sometimes incorrectly display the crossover interface that is being used.
Extreme Security	IV79078	The '/' partition on data nodes can sometimes run low of free disk space during new data node rebalancing.
Extreme Security Vulnerability Manager	IV79199	Asset updates from Vulnerability Manager scans might not occur during an Extreme Security auto update function.
Extreme Security Vulnerability Manager	IV79213	Loading **manage vulnerabilities** > **by asset** page can appear to hang or take a long time to load.
Extreme Security	IV79214	Netflow and ipfix data can sometimes be not fully processed and qflow 'src_mac' exceptions are visible in Extreme Security logging.
Extreme Security	IV79233	'Remote method error' pop up when searching on mac addresses where the mac data values are separated by a hyphen ' - '.
Extreme Security	IV79342	Extreme Security log activity graphing appearance is inconsistent depending upon the time frame selected.
Extreme Security	IV79345	Adding a regex filter to a search can generate error 'fatal exception in validationexception: this is not a valid...'.

6 Release Notes for ExtremeSecurity V7.7.2.6 Patch 2

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.6 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 7.7.2.6 Build 20160121152811.

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 7.7.2.5 to 7.7.2.6, see the *Extreme Networks Security Upgrade Guide*.

Resolved Issues

Product	Number	Description
ExtremeSecurity	IV78301	ECS-EC SERVICE DOES NOT GET RESTARTED AFTER A FULL DEPLOY AND/OR LICENSE CHANGE DEPLOY FUNCTION
ExtremeSecurity	IV79235	LOG FILE COLLECTION FROM THE USER INTERFACE CAN SOMETIMES FAIL AND RETURN ERROR '...CAN'T FIND RESULT FILE NAME...'
ExtremeSecurity	IV79607	ARIEL SAVED SEARCH RESULTS MIGHT NOT BE SYNCRONIZED TO HIGH AVAILABILITY CONSOLE SECONDARIES
ExtremeSecurity	IV79646	MESSAGE DURING PATCHING PROCESS 'USE OF UNINITIALIZED VALUE $IP IN CONCATENATION (.) OR STRING AT HASYSTEMCALLS.PM...'
ExtremeSecurity	IV80831	REPORTS CONTAINING TABLE CHARTS CAN IMPROPERLY DISPLAY THE VALUE FOR 'NONE'.
Extreme Networks Security Vulnerability Manager	IV79652	APPLICATION ERROR WHEN ATTEMPTING TO EDIT VULNERABILITY MANAGER SCAN PROFILE
Extreme Networks Security Vulnerability Manager	IV79705	VULNERABILITY 'LAST SEEN' DATE/TIME STAMPS CAN BE INCORRECT BY UP TO TWO HOURS IN SOME SITUATIONS
Risk Manager	IV78980	CISCO ASA CONFIGURATION BACKUPS CAN SOMETIMES FAIL WITHIN RISK MANAGER

Product	Number	Description
Multiple	SECURITY BULLETIN	VULNERABILITY IN MD5 SIGNATURE AND HASH ALGORITHM AFFECTS SIEM, AND INCIDENT FORENSICS (CVE-2015-7575)
Multiple	SECURITY BULLETIN	OPENSSL AS USED IN SIEM IS VULNERABLE TO A DENIAL OF SERVICE ATTACK, AND SENSITIVE INFORMATION EXPOSURE. (CVE-2015-3194, CVE-2015-3195, CVE-2015-3196)

7 Release Notes for ExtremeSecurity V7.7.2.6 Patch 1

Extreme Networks is pleased to introduce the ExtremeSecurity V7.7.2.6 Patch 1.

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 7.7.2.6 Build 20160106113021.

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 7.7.2.5 to 7.7.2.6, see the *Extreme Networks Security Upgrade Guide*.

Resolved Issues

This patch release adds app upgrade functionality to ExtremeSecurity. Updates to the GUI Application Framework API means you can upgrade apps that are installed on your ExtremeSecurity system without any loss of application data. You no longer need to uninstall the previous version before you update an app from the X-Force Exchange website. The framework now also handles upgrade failures, where the original app version is reinstated and you do not lose any application data if an upgrade issue occurs.

8 Release Notes for ExtremeSecurity V7.7.2.6

Extreme Networks Security Analytics V7.7.2.6 provides new features and fixes to known issues. For installation instructions, see the *Extreme Networks Security Installation Guide*.

New Features

What's new for administrators in V7.7.2.6:

- Deploy and manage multitenant instances of ExtremeSecurity—As a Managed Security Service Provider (MSSP) or a service provider within a multi-divisional organization, you can now deploy multitenant instances of IExtremeSecurity. By creating domains and tenants for each customer, you can manage each customer independently and ensure that data is visible only to the users of each tenant.
- Sharing and collaboration of ExtremeSecurity content on the Security App Exchange portal—The Security App Exchange is a new web portal for users and business partners to leverage the power and knowledge of the global community. Use the Security App Exchange to collaborate with others and to share security content in small, consumable extensions to enhance existing functionality in the ExtremeSecurity framework.
- Hide sensitive data directly from ExtremeSecurity—Use the new Data Obfuscation Management tool to hide sensitive data directly from ExtremeSecurity without using the command-line. The new pre-defined, field-based expressions make it easier to mask common data elements such as user names, group names, netBIOS names, and host names. You can also create regular expressions to obfuscate other data in the event and flow logs as required by your corporate and local government privacy policies.
- Import extensions and content without using the content management script—To extend the capabilities of ExtremeSecurity, use the new Extensions Management tool to import security extensions into your deployment. The new interface makes it easy for you to add and install applications and security content directly from the new Security App Exchange into ExtremeSecurity. Before you install an extension, you can review the content and specify whether existing content is overwritten or preserved.
- Deployment visualization—You can open a visualization of your deployment at the host level from the Deployment Actions list. In the visualization, you can see the relationship between your hosts and modify the relative location of hosts, without modifying the actual deployment configuration. You can also export the graphic in either PNG or VDX format.

- Multiple email notification templates—You can now select from a list of available response email templates when you are configuring rules. You can now create different templates for different users, different templates for different types of offenses, and so on. For more information about configuring rules, see the *Extreme Networks SIEM Users Guide*.
- Reference data expiry events—Elements from Reference Data Maps, Map of Sets, Map of Maps, Reference Table, and Reference Sets now trigger a Reference Data Expiry event when they expire. The Reference Data Expiry event contains the name of the collection and the element that expired. You can use the feature, for example, to track such things as expired user accounts on your network.
- Custom action scripts—You can attach scripts to custom rules that do custom actions in response to network events. For example, you can write a script to create a firewall rule that blocks a source IP address from your network in response to a rule that is triggered by a defined number of failed login attempts. You can use the Custom Action window on the Admin tab to manage custom action scripts.
- Improved security for system settings—Configure system settings in a new and more secure interface. Access the new View and Manage System window through HTTPS to configure firewalls, network interfaces, and email servers.

Note

To improve security, you configure system time and password changes in the ExtremeSecurity console.

- Inactivity timeout—The Inactivity Timeout property controls the maximum amount of time that an inactive session remains alive. If more than the specified time interval passes with no activity, the session is ended and you are logged out. By default, the maximum time interval is 30 minutes.

What's new for users in V7.7.2.6:

- Optimized indexes that speed search performance—In previous releases, indexes were created for each 1-minute interval. Now, with Super Indexes in ExtremeSecurity V7.7.2.6, the index data structure is optimized and a single super index is created at the end of each hour. For multi-hour searches in particular, ExtremeSecurity now scans the index more optimally, resulting in an up to 10x performance increase for Indicator of Compromise (IOC) type searches. Some examples of IOC type searches are searches on IP address, domain and host name. All new data that is received by ExtremeSecurity is automatically indexed in the new format.
- New CRE tests—A new custom rule engine (CRE) test is available to compare one property against another, including custom properties. You can now compare a source IP address against a destination IP address. You can compare a user name against a custom property.

  Use AQL WHERE clause grammar to build complex comparisons in the custom rules engine (CRE). You can use AND/OR logic, reference container lookups and asset model queries. You type only the conditions when you build your WHERE clause.
- License enhancements—ExtremeSecurity V7.7.2.6 changes the way that events affect your license. In previous releases, all events that were generated by ExtremeSecurity, such as EPS notifications, system notificaitons, and internally generated logs, were counted against your license. Now, the following internal events do not count toward your license:
  - system notifications
  - custom rule engine (CRE)
  - audit
  - ADE

- asset profiler
- results from scheduled searches
- health metrics
- Risk Manager questions, simulations and internal logging.

Only events that are generated on devices on the customer premise count toward your license. Also, 60% of events that you drop by using routing rules are credited back, up to a maximum of 2000 events per second (EPS).

- Viewing reference sets in rules and search results—You now have more access to data. Reference set information was previously unavailable to you if you didn't have Administrator privileges. Administrators can now grant access to you so that you can view reference sets in search results, and in common rules. You can now include reference sets in searches and common rules. You can view lists of reference sets, the contents of reference sets, and can export reference sets.
- Quick Filter in the right-click menu—The right-click menus now include a Quick Filter option for events and flows. Use the Quick Filter criteria to pivot data during your investigations. You can search on items that match, or don't match your selection. After you add the match/not match filter, more search criteria become available in the right-click menu.
- Improved query workflow to provide faster access to data—

  ExtremeSecurity improves the way that you interact with data and also lets you quickly expand the time before and after an offense occurred. Use the options for time series charts on the Network and Log activity tabs to quickly change the displayed time period, without leaving the activity view. For example, if you are investigating an offense that occurred on an endpoint at 4:30 PM on Tuesday, you can drill into the events from the offense itself. You can look at what happened a few minutes before or later the time span that you are looking at without having to open the Edit Search page. You can specify a time period, down to the minute, or expand a time period from the drop-down list.
- Historical correlation enhancements—ExtremeSecurity V7.7.2.6 introduces better visibility into threats and management of historical correlation profiles and results:
- Increased visibility of real threats—In ExtremeSecurity V7.7.2.5, historical offenses were created for any rule that was triggered during a historical correlation run. In V7.7.2.6, historical offenses are created only when the triggered rule specifies that an offense must be created for the detected event.
- Improved auditing—Audit records are created each time a historical correlation profile is run or canceled. This change provides you with improved monitoring and increased visibility to see which users are running or canceling historical correlation runs.
- New offense search capabilities—You can now search for offenses that were created from a selected historical correlation profile. You can also exclude historical correlation results from saved searches. With these new search parameters, you can separate historical correlation offenses from real-time offenses for reporting.
- Improved historical correlation profile management—Depending on the volume of historical data that you are processing and the criteria that you specify, you might find that the correlation takes a long time to complete. You can now cancel historical correlation profiles that are running or queued to run.

  You can sort and filter columns in the Historical Correlation window to easily find the information that you are looking for.

When you view the run history for a profile, you can quickly see the number of offenses that were created by a run. With a single-click, you drill down on the historical correlation catalogs to see the list of events or flows that matched the profile criteria.

- New AQL string and statistical functions— Use the following Ariel Query Language (AQL) functions in advanced searches when you want to find the position of a string or replace a string in a regular expression:

Function	Description
strpos	Returns the position of string inside another string.
regex_replace	Replaces a string by using a regex as the search condition.
first	Returns the first instances of the specified column.
last	Returns the last instances of the specified column.
stddev	Returns the sample standard deviation.
stddevp	Returns the population standard deviation.

For more information, see the Supported Functions section in the *Extreme Networks Security Ariel Query Language Guide*.

What's new for Risk Manager users:

- Topology screen enhancements—Manage and organize the topology graph by grouping devices, renaming devices, filtering the number of subnets that are displayed per device, showing or hiding unclassified devices. You can manage the density of network nodes that are displayed by filtering devices and subnets to form an uncluttered graph.
- Filtering device rules by user or group—To help you manage and optimize your network rule policies, you can view, filter, and search your device rules by user or group.
- Adapter integrations—Risk Manager introduces two new adapter integrations that extend the network devices that are supported, such as firewalls, routers, and switches that can be interrogated.
- Sidewinder adapter—Risk Manager adapter for Sidewinder supports McAfee Enterprise Firewall (Sidewinder) appliances that run SecureOS.
- TippingPoint adapter—Risk Manager adapter for TippingPoint supports TippingPoint appliances that run TOS and are under SMS control.

For more information, see the *Extreme Networks Security Risk Manager Adapter Configuration Guide*.

What's new for Vulnerability Manager users:

- Improve your security posture by integrating IBM's BigFix with Vulnerability Manager—Use Vulnerability Manager with BigFix® to identify high priority vulnerabilities, and determine which ones need to be fixed first. Fixlets are out-of-the-box packages that you can deploy to remediate specific vulnerabilities. Vulnerability Manager can automatically publish high priority vulnerability data to the BigFix Dashboard. Users can easily monitor and remediate Vulnerabilities from BigFix that are prioritzed by Vulnerability Manager.
- Support for multi-domain environments—Use the security profile permissions at the domain-level to ensure that the correct level of access is in place for vulnerability scans. You can now associate a scanner with a domain, use a domain for dynamic scanning, associate a domain with a scan profile

and scan result, see the assets in a domain that are associated with a scan, filter scan reports by domain, and see only the scan results and vulnerabilities that are in the domains that are associated with your security profile.

Announcement

The ExtremeSecurity V7.7.2.6 announcement is available by searching for your product on the Offering Information page. See the announcement 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 *Extreme Networks Security Installation Guide*.

Fix List

The following issues were corrected in ExtremeSecurity V7.7.2.6.

Number	Description
IV54477	During the reboot phase of a ExtremeSecurity upgrade, the system might hang due to multiple SSH sessions
IV61182	Message "java.lang.illegalargumentexception" when trying to filter on connection type
IV61296	Report time zone defaults to first value (GMT-11) for various time zones
IV69344	Hostservices sometimes does not restart the IMQ process
IV69368	Search parameter value fields currently have a maximum 255 character restriction
IV69371	Manually created network hierarchy object named 'other' will not display in rules
IV69642	Asset search filter 'add filter' not working as expected
IV70531	Custom rules no longer fire after switching an event rule to a common rule
IV70532	Clean assets with port vulnerabilities setting is worded incorrectly
IV70533	AQL: 'where' clause ordering affects time range limiters (start and stop)
IV70632	The 'category' selection in the rule wizard is not consistent with the rest of the UI
IV70661	Reference sets populated with ExtremeSecurity field like "event name" and "log source" cannot be used in rules or filters properly
IV7082	Exporting offenses to CSV format can cause the "allnotes" field to parse incorrectly
IV71188	Multiple unique SAR notifications from certain system events can get grouped into 1 event
IV71205	ExtremeSecurity UI may incorrectly return message 'Data re-balancing is complete with errors' while the logs indicate it is not complete
IV71208	Improper regex for default 'flow source' custom property
IV71506	Updating a console with a public IP address causes deployment editor to no longer save changes

Number	Description
IV71766	Modifying the ariel hashing algorithm requires two full deploys to take effect
IV72519	Generated offense emails contain incorrect 'last observed' date of '1 Jan 1970'
IV72676	Store and forward collector is unable to load the bandwidth limiting rules after patching
IV72738	User locale setting resets to ExtremeSecurity default (English) after user role change
IV72888	Error when performing ExtremeSecurity advanced searches when ordering by "Byte" column
IV72903	System notification error 'Out of memory discovered for host context' during backup process
IV72919	ExtremeSecurity Incident Forensics - PCAP appliance 'network throughput graph' shows larger than expected fluctuations
IV72922	Calculation-based custom event property fields are not displayed in the flow and event detail pages
IV73026	ExtremeSecurity Incident Forensics - Creating more than 40 cases in Case Management generates errors in the forensics.log file
IV73207	Global view configuration persists after global view is deleted causing unexpected results
IV73343	Searches that include comma separated IP addresses as a filter fail with error "There was a problem performing the query..."
IV73345	Changes made to displayed column and saved as a new asset quick search are not honored on subsequent asset pages
IV73479	Unable to delete a reference set
IV73510	Generated report pie charts display an alphanumeric string in the legend
IV73598	'NetBiosGroup' asset updates are not occurring
IV73625	Performing a full deploy interrupts ExtremeSecurity searches that are in progress
IV73630	Searching for a log source by name requires clicking the 'Go' button
IV73697	'Parse error...' message pop up when logging out of the ExtremeSecurity user interface
IV73915	"illegalstateexception" error observed in ExtremeSecurity logging after saving a log source
IV73916	"qidmapfactory" error observed in ExtremeSecurity logging after full deploy or other ECS service restart
IV74029	ExtremeSecurity allows system boot up using the recovery partition without requiring authentication
IV74082	Restoring a configuration backup that was taken from a ExtremeSecurity NAT environment to a non-NAT environment fails
IV74103	On demand ExtremeSecurity configuration backups do not start if scheduled configuration backups are disabled
IV74152	If 128 or more user roles have been created, some users may appear to have the Admin role in user details dropdown
IV74154	Performing a partial configuration restore that includes assets can fail on asset vulnerability information
IV74229	X-Force rules might be classified as expensive custom rules
IV74286	Log source reports might not include child log sources from selected parent log source groups

Number	Description
IV74397	Store and forward appliances (15xx) memory tunings can cause ECS-EC to run out of memory
IV74552	'Send feedback' check box does not work as expected
IV74555	"Please try again' from hosts with encryption enabled
IV74559	Searches that include search filters containing an IP address with a preceding or trailing blank space do not return results
IV74894	Content management tool (CMT) fails to import reference data of type 'string' that begins with a numeral
IV74956	High availability configuration restore can fail with error 'Backup from a non-HA standby system cannot be restored...'
IV75075	The 'test group' drop down menu of the rule wizard: rule test stack editor displays 'network property tests' twice
IV75109	Offense email responses do not work due to the alert-config.xml file being emptied
IV75112	Creating a high availability pair can fail when the appliance hostname(s) are longer than 54 characters
IV75203	Repeated QRadar.error logging of '[Warn] no PID file /store/tmp/status/qflow.pid yet]
IV75920	'Send to forwarding destination' rule response is not an available option for flow and offense rules
IV75957	Changes in how ExtremeSecurity creates tunnels can cause deployment failures if configured with an encrypted offsite console
IV75958	Deployments fail and hostcontext won't start after using qchange_netsetup with a bonded management interface
IV76161	Error during appliance boot '...prepare_io_scheduler: line 22: echo: write error : invalid argument'
IV76217	Error 'Host already exists in server host table' when attempting to add a high availability secondary
IV76403	ExtremeSecurity login attempts can create duplicate user profiles when LDAP group authorization is configured
IV76406	Assets that have multiple operating systems defined and have scan vulnerabilities identified can cause 'stored' events
IV77431	Authentication token information might not be restored after performing a configuration backup restore
IV77644	'Assetuser' and 'assethostname' functions generate errors when using ariel_query or api_client from the ExtremeSecurity backend
IV77924	Some ExtremeSecurity Incident Forensics integrated console logging is being written to the incorrect log file
IV78408	Running concurrent searches on a ExtremeSecurity appliance that is experiencing heavy load can cause nullpointerexceptions
IV78479	Performing quick filter searches can sometimes return an error 'The server encountered a file access error'
IV78537	Historical correlation can cause generated offenses for rules without offense rule responses

Known Issues

Issue description	Workaround
While trying to access Extreme Security Vulnerability Manager, the following application error is produced “- tomcat-rm trying to connect to incorrect ariel port”.	1 Run the following from the Vulnerability Manager command line:`service hostcontext sigquit` 2 Reboot QRM. 3 Perform a full deploy.
While trying to install multiple applications simultaneously to the Application Framework, some may not install successfully and produce errors.	Try to only install one app at a time. If required, a maximum of three apps may be installed simultaneously.
As a tenant admin, if you are trying to add a manual asset within the cidr range from the network hierarchy, you will get a “Failed to add asset” error message.	1 Instead of "Net-10-172-192", specify "Net-10-172-192/Net_172_16_0_0" in the security profile for the tenant admin. 2 Perform a full deploy.
The number of threads in the tomcat connection pool increases with the install, and uninstall of new apps. The increase may be up to 10 threads per app being installed.	Restart tomcat.
While trying to upgrade an existing app within the Application Framework, a new instance of the application will be created instead of upgrading the existing one.	1 Run the `upgrade_app.sh` script in the `/opt/qradar/bin` directory. For further information on using the upgrade script, see the developerWorks wiki.