ExtremeCloud™ Orchestrator v3.8.0 Release Notes

New Features, Supported Platforms, and Known Issues

9039188-00 Rev AA
April 2025

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, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

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

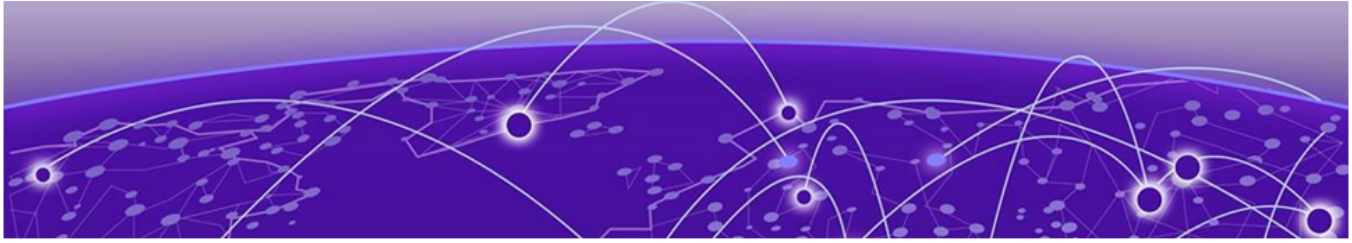
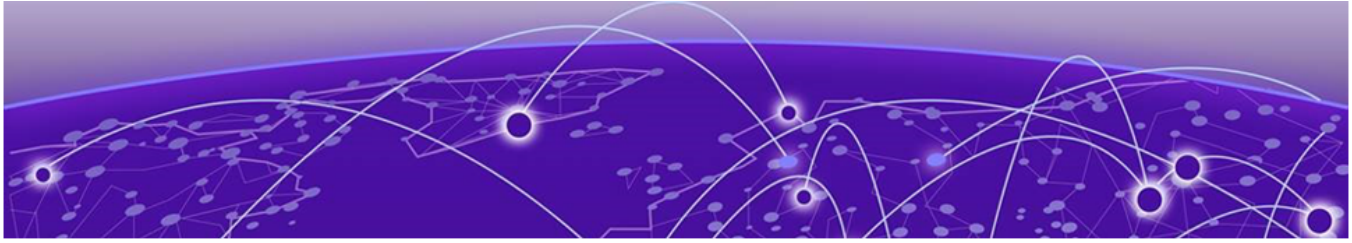
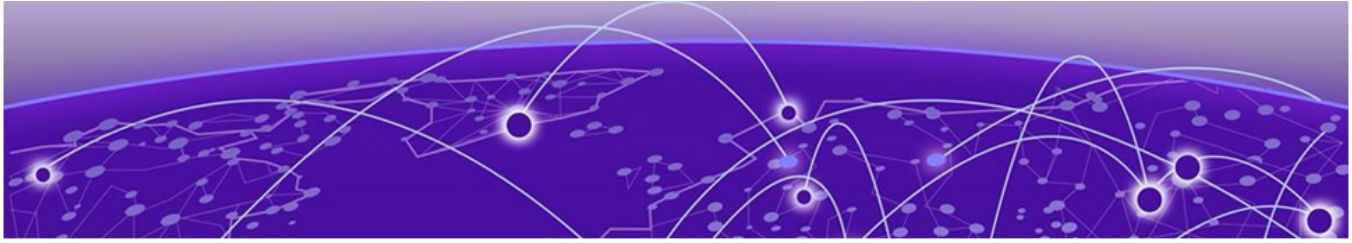


Table of Contents



Abstract

ExtremeCloud™ Orchestrator version 3.8.0 introduces several new features and enhancements, including retaining route-target configurations on border leaf devices, updated support matrices for fabric and visibility skills, and user interface updates. Supported deployment models encompass server, Open Virtual Appliance (OVA), and TPVM, with detailed specifications for each, including CPU, storage, and RAM requirements. Upgrade prerequisites include ensuring no DNS configuration exists under TPVM config and resolv.conf, and maintaining management connectivity from SLX and TPVM to external build server images. Numerous defects were addressed, such as BGP peer deletion errors and firmware version discrepancies, while open defects include issues like device discovery limitations and configuration drift in dynamic peers. Security patches address vulnerabilities in components like local-path-provisioner, Coredns, and raetrafik. For support, users are directed to Extreme Networks' various customer service channels.



Release Notes

New In This Release

ExtremeCloud Orchestrator 3.8.0 introduces the following features and enhancements, and resolves issues through defect fixes. For information about XCO deployment, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.8.0*.

Note
In release 3.2.0 and later, Extreme Fabric Automation (EFA) is referred to as ExtremeCloud Orchestrator (XCO). The terms EFA and XCO refer to the same product and are used interchangeably.

Table 1: Features and Improvements

Feature	Description
New and modified commands	New commands: • efa system security-banner reset • efa system security-banner set • efa system security-banner show • efa system security-banner unset • efa system ssh-key delete • efa system ssh-key export • efa system ssh-key generate • efa system ssh-key show Modified commands: • efa inventory device secure settings update • efa system feature update • efa system settings update • efa system supportsave • efa notification subscribers add-https • efa notification subscribers add-syslog-relp For more information, refer to the *ExtremeCloud Orchestrator Command Reference, 3.8.0*.
Configure Login Banner	• New topic "Login Banner" provides a detail description on login banner. • New topic "Configure System-Wide Banner" describes a procedure to configure a banner text. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.
Alarms and manual renewal	New topic "Alarms for Auto Certificate Renewal Failure" describes the generated alarms when the certificate renewal fails. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.

Table 1: Features and Improvements (continued)

Feature	Description
Supportsave Enhancements	New topic "Supportsave Enhancements" describes delimiters to encapsulate command outputs when collecting CLI results. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.
Passwordless SSH or SCP support for Backup and Log Files	New topics describe configuration details of SSH key-based passwordless authentication For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.
Bulk support for Tenant EPG APIs	• New topic "Bulk Support for Tenant EPG API" describes about the support. • New topic "Limitations" describes the limitations of bulk support for Tenant EPG API New topic "Enable Bulk Support for Tenant EPG APIs" describes the procedure to enable or disable bulk support for tenant EPG APIs. • New topic "Prerequisites for Bulk EPG Creation using APIs" describes the prerequisites for bulk EPG creation using API. • New topic "Configure EPG in Bulk using API" describes EPG configuration procedure in bulk using API. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.
Security event logging configuration	New topics "Security Event Logging Configuration" and "Validate Security Event Logs" describe and provide procedures to validate the event logging. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.
Configure Description on Device Interface	Updated the existing topic "Configure Description on Device Interface" with the details on creating custom descriptions for Ethernet ports and link aggregation groups on SLX devices. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.

Table 1: Features and Improvements (continued)

Feature	Description
Behavior change in setting admin state and description	Updated the existing topics "Change the Admin Status of an Interface" and "Configure Description on Device Interface" to reflect that the inventory service will now be solely responsible for managing admin state and description settings for Ethernet interfaces. For more information, refer to the *ExtremeCloud Orchestrator CLI Administration Guide, 3.8.0*.
System Hardening for CIS-CAT Assessments	CIS-CAT Assessments system hardening updates. For more information, refer to the *ExtremeCloud Orchestrator Security Configuration Guide, 3.8.0*.
Support Matrix	Updated the support matrices for supported platforms and deployment models for fabric and visibility skills. For more information, refer to the *ExtremeCloud Orchestrator Deployment Guide, 3.8.0*.
Packet Capture (PCAP)	Enhanced functionality for PCAP: • Simplified PCAP operation on Extreme 9920 Devices. • Time-event based PCAP Capture for Extreme 9920 Devices For more information, refer to the *ExtremeCloud Orchestrator GUI Administration Guide, 3.8.0*.
Support Save	Introduction of choice of User, Digital Certificate, or SSH Key based Authentication for Remote Servers. For more information, refer to the *ExtremeCloud Orchestrator GUI Administration Guide, 3.8.0*.

For other additional information, see Defects Closed with Code Changes on page 14.

Supported Platforms and Deployment Models for Fabric Skill

Support includes Server, Open Virtual Appliance (OVA), and TPVM deployment models, supported TPVM versions, supported SLX-OS software versions, and supported SLX devices.

Note

- OVA deployment model does not support HA.
- As a best practice, refer to the following Extreme validated support matrices for supported platforms and deployment models information.

Table 2: Server Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Server Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	More than 24	Yes	18.04 LTS and 20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x, 3.8.x	More than 24	Yes	20.04 LTS and 22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 3: OVA Deployment Models

XCO Version	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	More than 24	Yes	20.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x, 3.8.x	More than 24	Yes	22.04 LTS	• CPU: 4 cores • Storage: 64 GB • RAM: 8 GB

Table 4: TPVM Deployment Models

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
3.4.x, 3.5.x, 3.6.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520	Up to 24	Yes	20.04 LTS	20.5.2a

Table 4: TPVM Deployment Models (continued)

XCO Version	TPVM Deployment	Managed SLX Devices	Multi-Fabric Support	Ubuntu Version	Minimum SLX-OS Version
	• Extreme 8720 • Extreme 8820 (20.4.3 and later)				
3.7.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	22.04 LTS	20.6.3a
3.8.x	• SLX 9150 • SLX 9250 • SLX 9740 • Extreme 8520 • Extreme 8720 • Extreme 8820 (20.4.3 and later)	Up to 24	Yes	22.04 LTS	20.7.1

Table 5: TPVM Software Support

XCO Version	TPVM Version	SLX-OS Version
3.4.0	4.6.6	20.5.3a
3.4.1	4.6.7	20.5.3a
3.4.2	4.6.8	20.5.3a
3.5.0	4.6.10	20.6.1
3.6.0	4.6.13, 4.6.14	20.6.2, 20.6.2a
3.7.0	4.6.17, 4.7.0	20.6.3a
3.8.0	4.7.4	20.7.1a

Table 6: IP Fabric Topology Matrix

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
	20.3.x, 20.4.x	Yes	Yes	Yes	Yes	Yes

Table 6: IP Fabric Topology Matrix (continued)

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
Extreme 8720						
Extreme 8520	20.3.x, 20.4.x	Yes			Yes	Yes
Extreme 8820	20.4.3		Yes		Yes	Yes

Supported Platforms and Deployment Models for Visibility Skill

Support includes Server, OVA, and supported devices and software.

Note

- Upgrade from XVM (Extreme Visibility Manager) to XCO is not supported.
- XCO supports only a fixed set of special characters for hostnames. Any additional characters configured in MLX or SLX are reconciled in XCO and can be edited or deleted. Any configuration name must start with an alphanumeric character and can contain a-z A-Z 0-9 _ -.

Table 7: Ubuntu Server Version

XCO Version	Ubuntu Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	18.04 LTS and 20.04 LTS	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB
3.7.x, 3.8.x	20.04 LTS and 22.04 LTS	Minimum: • CPU: 4 cores • Storage: 128 GB • RAM: 8 GB Recommended: • CPU: 16 cores • Storage: 200 GB • RAM: 32 GB

Table 8: OVA Deployment Models

XCO Version	Ubuntu Version	Virtual Machine
3.4.x, 3.5.x, 3.6.x	20.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB • RAM: 8 GB
3.7.x, 3.8.x	22.04 LTS	Minimum: • CPU: 4 cores • Storage: 64 GB

Table 8: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
		• RAM: 8 GB

Table 9: Supported Devices and Software

Device	Supported Software
Extreme 9920	Extreme 9920 software with the NPB application • 21.1.2.x • 21.2.1.x • 21.2.2.x
Extreme Routing MLX Series	• NetIron 6.3.00 patches
Extreme Switching SLX 9140	• SLX-OS 18s.1.03 patches
Extreme Switching SLX 9240	• SLX-OS 18s.1.03 patches

XCO Upgrade Prerequisites

Prerequisites for XCO upgrade process with the default gateway changed:

1. Ensure that no DNS configuration exists under TPVM config and resolv.conf.
2. Presence of management connectivity from SLX and TPVM to external build server image, wherein image is available during SLX and TPVM upgrade process.

If file/etc/sshd/sshd_config is modified to non-default values, then manually readjust the following parameters:

- MaxStartups 30:30:100
- MaxAuthTries 6
- LoginGraceTime 120

Note
The hardening script, extr-granite.py bundled with EFA 2.6.1 will not automatically modify the above mentioned parameters.

Defects Closed with Code Changes

The following defects were closed in this release.

Parent Defect ID:	XCO-9216		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.3.0
Symptom:	Causing multiple subscription on devices, leading to memory leak.		
Condition:	When one of the device is in unhealthy state.		

Parent Defect ID:	XCO-9769		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.1
Symptom:	Unable to delete the prefix list from Policy Service, even though it is not bound to the tenant service.		
Condition:	After deleting the ipv6 prefix from bgp-peer in tenant service, unable to delete prefix-list from policy service.		
Recovery:	Use the following CLI command: 1) efa inventory device update --ip <>		

Parent Defect ID:	XCO-9942		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	Few POs will remain on SLX Devices and Few POs will remain in XCO database after executing EPG delete and PO delete in quick succession. [Two commands executed at same time]		
Condition:	Few POs will remain on SLX Devices and Few POs will remain in XCO database after executing EPG delete and PO delete in quick succession. [Two commands executed at same time]		
Workaround:	Delete EPG and wait for the profile to be applied on the PO and then delete the PO after ensuring EPG delete is complete.		
Recovery:	GO to SLX device and Remove the POs manually and do inventory device update.		

Parent Defect ID:	XCO-10461		
Product:	XCO Visibility Skill	Reported in Release:	XCO 3.5.0
Symptom:	Display wrong date post refresh pcap file.		
Condition:	Post performing refresh operation.		

Parent Defect ID:	XCO-10461
Workaround:	Do not press refresh icon.
Recovery:	Refresh again to see the correct date.

Parent Defect ID:	XCO-10565		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	When the SLX switch is replaced, the cluster ports are correctly listed on XCO. But unbinding the profile from qos-policy fails.		
Condition:	When the SLX switch is replaced, the cluster ports are correctly listed on XCO. But unbinding the profile from qos-policy fails.		

Parent Defect ID:	XCO-10585		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.2.1
Symptom:	When creating mirror session in XCO, an error message is seen as ' service is not available or internal server error has occurred, please try again later'.		
Condition:	Create mirror session fails.		

Parent Defect ID:	XCO-11053		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	The command 'efa inventory device setting update' accepts same range of values for the --crypto-cert-expiry levels Info, Minor, Major and Critical		
Condition:	While running the command 'efa inventory device setting update', the flags --crypto-cert-expiry-info, --crypto-cert-expiry-minor, --crypto-cert-expiry-major and --crypto-cert-expiry-critical accepts values of range 0-90.		

Parent Defect ID:	XCO-11483		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.7.0
Symptom:	TPVM Hardening Script asks for user input to restart services		
Condition:	TPVM Hardening Script asks for user input to restart services		

Parent Defect ID:	XCO-10980		
	XCO Fabric Skill	Reported in Release:	XCO 3.7.0

Parent Defect ID:	XCO-10980		
Product:			
Symptom:	Description is not setting on the fabric ports, after set-description command.		
Condition:	When set-description command is used for setting the description for fabric ports, the description is not setting on the fabric ports interface.		

Open Defects

There following defects are open in this release.

Parent Defect ID:	XCO-8191		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.3.0
Symptom:	If you run concurrent epg update commands operation as port-group-add or vrf-add on bridge-domain EPGs that are associated with more than one ctag, one or some of the commands may fail with error "Save for device failed".		
Condition:	This is observed more often when more than 3 concurrent EPG port-group-add commands with non-conflicting ports and non-overlapping ctag-range are executed. Occasionally, configuration information that is pushed by one command is not used properly to prepare command recipe for another, causing the failure of one command.		
Workaround:	Rerunning the failing command will succeed. The error is intermittent and does not cause permanent changes. XCO state information is not affected at any point.		
Recovery:	No recovery is required as no state change is done as part of this failure.		

Parent Defect ID:	XCO-9363		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.0
Symptom:	After removing the tenant using the --force option, Fabric binding is not applied on the physical interfaces which were part of the port-channel/physical interfaces.		

Parent Defect ID:	XCO-9363
Condition:	Issue is observed when user issues the command 'efa tenant delete --name <tenant_name> --force'
Workaround:	User needs to unbind the policies (QoS) from all the relevant targets (fabric/tenant/port/port channel/tenant endpoint group) before executing the force operations including delete to avoid the stale policies(QoS) in the system.

Parent Defect ID:	XCO-10067		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.5.0
Symptom:	After adding border-leaf to the fabric, fabric-internal profile is not getting applied on the MCT port-channel.		
Condition:	After adding new devices(leaf/border-leaf) to the fabric followed by fabric configure, fabric-internal profile is not getting applied on the MCT Port-channel of the newly added devices(leaf/border-leaf).		
Workaround:	User can issue rebind the fabric internal port QoS profile using below command: Bind Fabric internal ports QoS profile: efa policy qos profile bind --name <profile_name> --fabric <fabric_name> --port fabric-internal.		

Parent Defect ID:	XCO-10339		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.6.0
Symptom:	Border leafs and spines are marked as "cfg-refreshed" error, along with "efa fabric error show" displayed as a CLOS error.		
Condition:	Below are the steps to reproduce the issue. 1. Create a 5-stage clos fabric. 2. Add super-spines, spines and border-leafs in a single pod. Border leaf is connected to super-spines and not connected to spine. 3. Configure the fabric. 4. Execute "efa backup and restore" or "border leaf reload".		
Workaround	User needs to make sure the spine is placed in a separate pod, border leaf is placed in a separate pod and super-spines are placed in a separate pod.		

Parent Defect ID:	XCO-10430		
	XCO Visibility Skill	Reported in Release:	XCO 3.6.0

Parent Defect ID:	XCO-10430		
Product:			
Symptom:	In the firmware history page, the previous and target versions are interchanged during the firmware restore operation. The same issue is also seen in the firmware history CLI response.		
Condition:	firmware restore operation on a 9920 device or a fabric SLX device from the GUI or CLI.		

Parent Defect ID:	XCO-10566		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.4.1
Symptom:	Configuring switchport mode trunk fails with netconf rpc error: 'Config not allowed as it will exceed system max allowed AC LIFs..',		
Condition:	Network Policy Error: Configuring switchport mode trunk on 27 failed due to netconf rpc [error] '%Error: Config not allowed as it will exceed system max allowed AC LIFs..' is seen while creating EPGs with high CTAG range and port channels		
Workaround:	When the EPG creation fails for high CTAG range, create it incrementally using medium/less CTAG ranges until the available limit is reached.		

Parent Defect ID:	XCO-11047		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.7.0
Symptom:	After upgrade and DRC, the description is not retained on interface		
Condition:	When the XCO is upgraded, description is not retained after DRC is done.		

Parent Defect ID:	XCO-11138		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.7.0
Symptom:	GoNotification pod will be missing from k3s after renewal of k3s server certificate even if it is not disabled before the command execution.		
Condition	Executing "efa certificate server renew" will lead the system to end up in an issue state.		
Recovery:	Execute the commnad "efa system service enable notification"		

Parent Defect ID:	XCO-11943		
	XCO Fabric Skill	Reported in Release:	XCO 3.8.0

Parent Defect ID:	XCO-11943		
Product:			
Symptom:	The base alpine container used in local-path-provisioner package is version 3.20.0 which has some known security vulnerabilities. Need to upgrade the container to latest version which is 3.20.3.		
Condition:	These security vulnerabilities are present in the older alpine container version 3.20.0 used in local-path-provisioner package. These are resolved in the newer 3.20.3 package of alpine.		

Parent Defect ID:	XCO-12497		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.8.0
Symptom:	The user won't be able to see the audit log at external servers.		
Condition:	It will appear with single-node OVA deployment for release 3.8.0 or greater.		
Workaround:	1. Replace and save the real OVA IP address in the placeholders as given below in the rsyslog configuration [/etc/rsyslog.d/40-raslog-tls.conf] template(name="SyslogProtocolRFC5424_Format" type="string" string="<%PRI%>1 %timegenerated:::date-rfc3339% <REAL_OVA_IP_ADDRESS> audit %procid% AUDITD_EVENTS - %msg%\n") if $programname == 'audisp-syslog' then { *.* @@<REAL_OVA_IP_ADDRESS>:6514;SyslogProtocolRFC5424_Format } 2. Restart the rsyslog service to apply the changes. systemctl restart rsyslog systemctl status rsyslog		

Parent Defect ID:	XCO-12611		
Product:	XCO Fabric Skill	Reported in Release:	XCO 3.8.0
Symptom:	The user won't be able to see the audit log at external servers.		
Condition:	XCO node reboot or HA post hardening script execution with version "0.97.2"		
Workaround:	1. Set "ForwardToSyslog" value to "yes" in journal config file [/etc/systemd/journald.conf] sed -i -e "s/ForwardToSyslog=no/ ForwardToSyslog=yes/" /etc/systemd/journald.conf 2. Restart the journald service to apply the changes. systemctl restart systemd-journald		

Security Patch

The following table lists the updated security components and vulnerabilities addressed in ExtremeCloud Orchestrator 3.7.1 and later releases.

Component	Previous Version	Latest Version	Vulnerabilities
golang	1.22	1.24	• GO-2023-2102 • GO-2023-2185 • GO-2023-2382 • GO-2024-2456 • GO-2024-2466 • GO-2024-2598 • GO-2024-2599 • GO-2024-2600 • GO-2024-2606 • GO-2024-2609 • GO-2024-2610 • GO-2024-2687 • GO-2024-2887 • GO-2024-2963 • GO-2024-3106 • GO-2024-3250 • GO-2025-3367 • GO-2025-3368 • GO-2025-3373 • GO-2025-3420 • GO-2025-3447 • GO-2025-3487
local-path-provisioner	0.0.28	0.0.30	• CVE-2024-45337 • CVE-2023-48795 • CVE-2024-45338 • CVE-2023-45288 • CVE-2024-24786 • CVE-2024-24790 • CVE-2023-45288 • CVE-2024-34156 • CVE-2023-39326 • CVE-2023-45289 • CVE-2023-45290 • CVE-2024-24783 • CVE-2024-24784 • CVE-2024-24785 • CVE-2024-24789 • CVE-2024-24791 • CVE-2024-34155 • CVE-2024-34158 • CVE-2024-45336 • CVE-2024-45341

Component	Previous Version	Latest Version	Vulnerabilities
local-path-provisioner	0.0.28	0.0.30	• CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-9143 • CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-9143

Component	Previous Version	Latest Version	Vulnerabilities
coredns	1.10.1	1.12.0	• CVE-2024-51744 • CVE-2024-45339 • CVE-2024-45337 • CVE-2023-48795 • CVE-2022-41723 • CVE-2023-39325 • CVE-2024-45338 • CVE-2023-3978 • CVE-2023-44487 • CVE-2023-45288 • CVE-2023-44487 • CVE-2024-24786 • CVE-2024-24538 • CVE-2024-24540 • CVE-2024-24790 • CVE-2022-41722 • CVE-2022-41724 • CVE-2022-41725 • CVE-2023-24534 • CVE-2023-24536 • CVE-2023-24537 • CVE-2023-24539 • CVE-2023-29400 • CVE-2023-29403 • CVE-2023-39325 • CVE-2023-45283 • CVE-2023-45288 • CVE-2024-34156 • CVE-2023-24532 • CVE-2023-29406 • CVE-2023-29409 • CVE-2023-39318 • CVE-2023-39319 • CVE-2023-39326 • CVE-2023-45284 • CVE-2023-45289 • CVE-2023-45290 • CVE-2024-24783 • CVE-2024-24784 • CVE-2024-24785 • CVE-2024-24789 • CVE-2024-24791 • CVE-2024-34155 • CVE-2024-34158 • CVE-2024-45336 • CVE-2024-45341

Component	Previous Version	Latest Version	Vulnerabilities
traefik	2.10.7	2.11.18	• CVE-2024-35255 • CVE-2024-41110 • CVE-2023-28840 • CVE-2023-28841 • CVE-2023-28842 • CVE-2024-24557 • CVE-2024-29018 • CVE-2024-28180 • GHSA-2c7c-3mj9-8fqh • CVE-2024-51744 • CVE-2024-6104 • CVE-2024-22189 • CVE-2023-49295 • CVE-2024-53259 • CVE-2024-45337 • CVE-2023-48795 • CVE-2024-45338 • CVE-2023-45288 • CVE-2024-24786 • CVE-2024-24790 • CVE-2023-45288 • CVE-2024-34156 • CVE-2023-45289 • CVE-2023-45290 • CVE-2024-24783 • CVE-2024-24784 • CVE-2024-24785 • CVE-2024-24789 • CVE-2024-24791 • CVE-2024-34155 • CVE-2024-34158 • CVE-2024-45336 • CVE-2024-45341

Component	Previous Version	Latest Version	Vulnerabilities
mirrored-library-traefik	2.10.7	2.11.18	• CVE-2023-42363 • CVE-2023-42364 • CVE-2023-42365 • CVE-2023-42366 • CVE-2024-4603 • CVE-2024-4741 • CVE-2024-5535 • CVE-2024-6119 • CVE-2024-2511 • CVE-2024-9143
erlang	25.3.2.15	27.2.4	• CVE-2024-12254 • CVE-2024-9287 • CVE-2024-12254 • CVE-2024-9287

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)

- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.