ExtremeCloud™ Orchestrator v3.8.8 Release Notes

New Features, Supported Platforms, and Known Issues

9039188-08 Rev AA
April 2026

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/

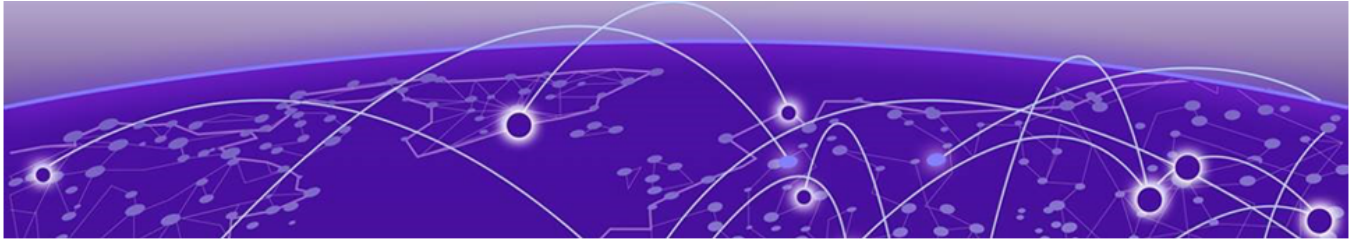
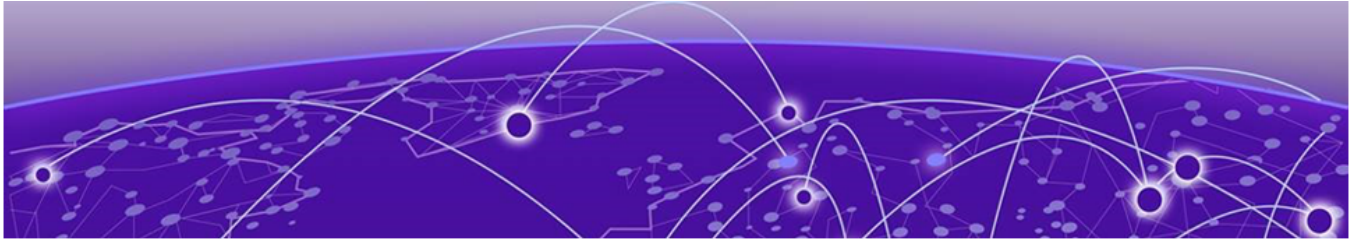
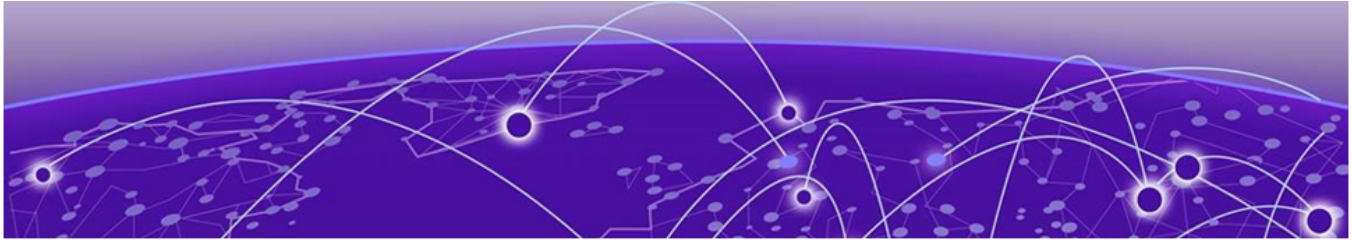


Table of Contents



Abstract

The release notes for ExtremeCloud™ Orchestrator version 3.8.8 presents a security-focused maintenance release that delivers critical updates to core orchestration components and addresses multiple CVEs. The document outlines supported deployment models—including Server, OVA, and TPVM—across validated Ubuntu and SLX-OS versions, with compatibility matrices for SLX and Extreme hardware platforms. Upgrade procedures emphasize DNS cleanup and persistent management connectivity. Visibility skill support, SSH hardening guidance, and hostname compliance rules are also covered. The content is tailored for technically proficient users managing multi-fabric orchestration in high-availability environments.



Release Notes

New In This Release

ExtremeCloud Orchestrator 3.8.8 resolves issues through a critical security patch. 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.

For more information, see Security Patch on page 11.

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 1: 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 2: 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 3: 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 3: 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 4: 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
3.8.1	4.7.5	20.7.1a
3.8.2	4.7.7, 4.7.9	20.7.1ab, 20.7.2ab
3.8.3	4.7.8	20.7.1ab
3.8.4	4.7.10	20.7.2ab
3.8.5	4.7.12	20.7.3a
3.8.6	4.7.13	20.7.3a

Table 4: TPVM Software Support (continued)

XCO Version	TPVM Version	SLX-OS Version
3.8.7	4.7.14	20.7.3a
3.8.8	4.7.15	20.7.3ab

Table 5: IP Fabric Topology Matrix

Device	SLX-OS Release	Leaf	Spine	Super Spine	Border Leaf	Small DC Fabric
SLX 9150	20.5.x, 20.6.x, 20.7.x	Yes	-	-	-	Yes
SLX 9250	20.5.x, 20.6.x, 20.7.x	Yes	Yes	Yes	-	Yes
SLX 9540	20.5.x, 20.6.x, 20.7.x	Yes	-	-	Yes	-
SLX 9640	20.5.x, 20.6.x, 20.7.x	-	-	-	Yes	-
SLX 9740	20.5.x, 20.6.x, 20.7.x	-	Yes	Yes	Yes	Yes
Extreme 8720	20.5.x, 20.6.x, 20.7.x	Yes	Yes	Yes	Yes	Yes
Extreme 8520	20.5.x, 20.6.x, 20.7.x	Yes	-	-	Yes	Yes
Extreme 8820	20.5.x, 20.6.x, 20.7.x	Yes	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 6: 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 7: 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 7: OVA Deployment Models (continued)

XCO Version	Ubuntu Version	Virtual Machine
		• RAM: 8 GB

Table 8: 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.

Security Patch

The following table lists the updated security components and vulnerabilities addressed in this release.

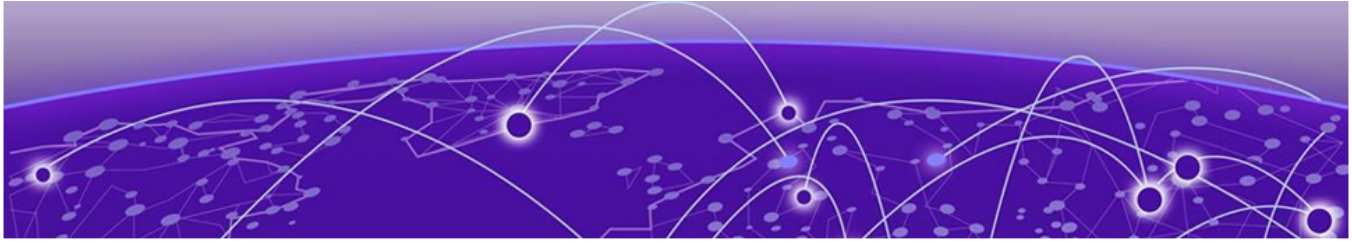
Component	Previous Version	Latest Version	Vulnerabilities
K3S Service	NA	NA	CVE-2025-15467 CVE-2025-68121 CVE-2025-61731 CVE-2025-61732 CVE-2025-69419 CVE-2025-69420 CVE-2025-69421 CVE-2025-11187 CVE-2025-15468 CVE-2025-15469 CVE-2025-61728 CVE-2025-61730 CVE-2025-66199 CVE-2025-68160 CVE-2025-69418 CVE-2026-22795 CVE-2026-22796 CVE-2025-68119 CVE-2026-24051 CVE-2026-25949 CVE-2025-47914 CVE-2025-58181 CVE-2025-15558 CVE-2026-22184 CVE-2026-26999 CVE-2026-29054 CVE-2026-34040 CVE-2026-33997 CVE-2026-32695 CVE-2026-33433 CVE-2026-26998 CVE-2026-27142 CVE-2026-29777 CVE-2026-27139 GHSA-9h8m-3fm2-qjrq GHSA-f6x5-jh6r-wrfv GHSA-j5w8-q4qc-rx2x GHSA-p436-gjf2-799p
Containers	NA	NA	CVE-2026-32767

Component	Previous Version	Latest Version	Vulnerabilities
			CVE-2026-23941 CVE-2026-23942 CVE-2026-23943 CVE-2026-32776 CVE-2026-32777 CVE-2026-32778 GHSA-34x7-hfp2-rc4v GHSA-3ppc-4f35-3m26 GHSA-5j98-mcp5-4vw2 GHSA-7h2j-956f-4vf2 GHSA-83g3-92jg-28cx GHSA-8qq5-rm4j-mr97 GHSA-r6q2-hw4h-h46w GHSA-73rr-hh4g-fpgx
Host Packages	NA	NA	CVE-2022-23806 CVE-2023-29404 CVE-2023-24538 CVE-2025-22871 CVE-2023-24531 CVE-2023-29405 CVE-2024-24790 CVE-2023-24540 CVE-2023-29402 CVE-2024-45337 CVE-2022-24675 CVE-2024-34158 CVE-2022-32189 CVE-2022-23773 CVE-2022-30632 CVE-2022-30633 CVE-2022-30635 CVE-2022-27664 CVE-2021-44716 CVE-2022-28327 CVE-2023-24534 CVE-2023-44487 CVE-2023-45288 CVE-2024-24784 CVE-2024-24791 CVE-2021-41771 CVE-2024-34156 CVE-2023-45287 CVE-2022-41723

Component	Previous Version	Latest Version	Vulnerabilities
			CVE-2023-24536 CVE-2023-24539 CVE-2022-41725 CVE-2023-39323 CVE-2022-30580 CVE-2021-41772 CVE-2023-45285 CVE-2023-29400 CVE-2022-30631 CVE-2022-30630 CVE-2022-2880 CVE-2025-61725 CVE-2025-61723 CVE-2022-41724 CVE-2022-24921 CVE-2022-23772 CVE-2022-41715 CVE-2022-2879 CVE-2022-28131 CVE-2023-24537 CVE-2025-58187 CVE-2025-47907 CVE-2023-29403 CVE-2025-58188 CVE-2025-4674 CVE-2025-22868 CVE-2025-22869 CVE-2022-27191 CVE-2023-45283 CVE-2023-39325 CVE-2022-41722 CVE-2022-41720 CVE-2022-41716 CVE-2022-30634 CVE-2022-29804 CVE-2021-43565 CVE-2024-27304 CVE-2024-27289 CVE-2024-24787 CVE-2024-24783 CVE-2023-45289 CVE-2023-45290 CVE-2023-29406

Component	Previous Version	Latest Version	Vulnerabilities
			CVE-2022-41717 CVE-2024-24785 CVE-2021-44717 CVE-2022-29526 CVE-2024-45336 CVE-2024-45341 CVE-2023-39326 CVE-2023-29409 CVE-2023-39318 CVE-2023-39319 CVE-2024-34155 CVE-2022-32148 CVE-2022-1705 CVE-2025-47906 CVE-2025-58186 CVE-2025-58185 CVE-2023-24532 CVE-2025-47912 CVE-2025-4673 CVE-2025-22866 CVE-2025-61724 CVE-2025-58183 CVE-2025-58189 CVE-2024-24789 CVE-2022-1962 CVE-2025-0913 CVE-2023-45284 CVE-2024-24786 CVE-2022-32149 CVE-2025-22872 CVE-2025-22870 CVE-2023-3978 CVE-2025-58181 CVE-2025-47914 CVE-2023-48795 CVE-2022-2582 CVE-2020-8911 CVE-2025-22873 CVE-2022-30629 CVE-2020-8912 GHSA-v778-237x-gjrc GHSA-6v2p-p543-phr9 GHSA-69cg-p879-7622

Component	Previous Version	Latest Version	Vulnerabilities
			GHSA-8c26-wmh5-6g9v GHSA-4374-p667-p6c8 GHSA-mrww-27vc-gghv GHSA-m7wr-2xf7-cm9p GHSA-hcg3-q754-cr77 GHSA-vvpx-j8f3-3w6h GHSA-69ch-w2m2-3vjp GHSA-gwc9-m7rh-j2ww GHSA-7jwh-3vrq-q3m8 GHSA-x6gf-mpr2-68h6 GHSA-m425-mq94-257g GHSA-qppj-fm5r-hxr3 GHSA-4v7x-pqxf-cx7m GHSA-45x7-px36-x8w8 GHSA-xrjj-mj9h-534m GHSA-8r3f-844c-mc37 GHSA-f5pg-7wfw-84q9 GHSA-p782-xgp4-8hr8 GHSA-vvgc-356p-c3xw GHSA-2wrh-6pvc-2jm9 GHSA-6jvc-q2x7-pchv GHSA-j5w8-q4qc-rx2x GHSA-qxp5-gwg8-xv66 GHSA-f6x5-jh6r-wrfv GHSA-7f33-f4f5-xwgw



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.