November 2026

Extreme TPVM 4.7.22

Release Notes

Supporting Extreme Routing and Extreme Switching SLX 9740, SLX 9640, SLX 9540, Extreme 8820, Extreme 8720, and Extreme 8520

9039146-22 Rev AA

© 2026, Extreme Networks, Inc. All Rights Reserved.

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 www.extremenetworks.com/company/legal/trademarks/. The hardware, firmware, software, or any specifications described or referred to in this document are subject to change without notice.

Contents

Release Overview 7
Security Update 7
New Features 7
Common Vulnerabilities and Exposures (CVEs) Addressed in this release 7
Changes in Behavior 9
Hardware and Software Support 9
Limitations and Restrictions 10
Upgrading TPVM to 4.7.22 10
TPVM package list 10
tpvm_sec_upgrade.sh script 11

Document History

Version	Summary of changes	Publication date
REV AA	Initial version for 4.7.22	November 2026

Preface

Getting Help

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, call (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.

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 Service Notifications

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

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form. All fields are required.
3. Select the products for which you want to receive notifications.
   Note: You can change your product selections or unsubscribe at any time.
4. Select **Submit**.

Extreme Resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at https://www.extremenetworks.com/support/documentation/.

Document Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. 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 we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

You can provide feedback in the following ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Release Overview

Release TPVM 4.7.22 does not provide any new features.

Security Update

- Security updates are included up to October 30, 2026.

New Features

- The hardening script is updated to latest version 0.97.13.

Common Vulnerabilities and Exposures (CVEs) Addressed in this release

The following CVEs are addressed in this release:

Fixed CVE(USN)	Package Name
CVE-2026-75029 CVE-2026-19666 CVE-2026-19662 CVE-2026-19941 CVE-2026-78301 CVE-2026-19033 CVE-2026-19667 CVE-2026-19668 CVE-2026-77119 CVE-2026-80274 CVE-2026-81563 CVE-2026-81736 USN-8929-1	bind9-dnsutils / bind9-host / bind9-libs (Needs evaluation)
CVE-2026-86409 CVE-2026-86414 CVE-2026-87862 CVE-2026-87864 CVE-2026-92388 CVE-2026-92389 CVE-2026-92391 CVE-2026-94266 USN-8932-1	curl
CVE-2026-16517 USN-8902-1	libarchive13
CVE-2026-54371 USN-8691-1	libattr1
CVE-2026-111497 USN-8956-1	libbrotli1
CVE-2026-69184 USN-8951-1	libc-ares2

CVE-2026-86409 CVE-2026-86414 CVE-2026-87862 CVE-2026-87864 CVE-2026-92388 CVE-2026-92389 CVE-2026-92391 CVE-2026-94266 USN-8932-1	libcurl3-gnutls, libcurl4
CVE-2026-95512 USN-8881-1	libfreetype6
CVE-2026-46675	libpng16-16
CVE-2026-16313 USN-8874-1	libsgutils2-2
CVE-2026-88806 CVE-2026-94283 CVE-2026-94284 CVE-2026-94285 USN-8913-1	libx11-6, libx11-data, and libx11-xcb1
CVE-2026-76781 CVE-2026-86138 CVE-2026-86142 CVE-2026-86143 CVE-2026-86144 USN-8910-1	libxml2
CVE-2026-94287 USN-8862-1	libxpm4
CVE-2026-94286 USN-8939-1	libxtst6
CVE-2026-106552 CVE-2026-106553 CVE-2026-106555 CVE-2026-106582 CVE-2026-106583 CVE-2026-106584 CVE-2026-106585 CVE-2026-106586 CVE-2026-106587 USN-8928-1	openssh-client, openssh-server, and openssh-sftp-server
CVE-2026-101917 CVE-2026-101918 CVE-2026-102274	python3-jwt

CVE-2026-102275 USN-8934-1	
CVE-2026-97689 USN-8926-1	python3-urllib3
CVE-2026-16313 USN-8874-1	sg3-utils ,sg3-utils-udev
CVE-2026-96512 USN-8895-1	sudo
CVE-2026-31715 CVE-2026-31712 CVE-2026-31711 CVE-2026-31709 CVE-2026-31700 CVE-2026-31451 CVE-2026-31449 CVE-2026-23364 CVE-2025-39931 CVE-2025-39929 CVE-2025-39863 CVE-2025-23131 CVE-2025-22026 CVE-2023-54271 CVE-2023-54125 CVE-2022-3114 USN-8875-1	linux/linux-image-generic

Changes in Behavior

The following are the behavioral changes for TPVM 4.7.22.

- None

Hardware and Software Support

- TPVM 4.7.22 supports the following hardware platforms: SLX 9540, SLX 9640, SLX 9740, Extreme 8520, Extreme 8720, and Extreme 8820.
- Minimum supported SLX-OS version for TPVM 4.7.22 is SLX-OS 20.6.3a.
- Full Install is required for upgrade and downgrade between TPVM versions lower than 4.7.0 and TPVM version 4.7.22.
  Note: Releases prior to TPVM 4.7.3 are not supported as per baseline-free upgrade.

Limitations and Restrictions

- Incremental upgrade is not supported between TPVM versions lower than 4.7.0 and TPVM version 4.7.22.
    - Example: Incremental upgrade and downgrade between TPVM 4.6.17 and 4.7.22 versions is not supported. If attempted, the following error message is displayed.
      Error: As Ubuntu LTS version is upgraded between the TPVM versions, incremental upgrade is not supported.
- TPVM incremental upgrade sometimes takes close to 30 minutes to complete. This time depends on the number of packages being updated. A temporary fix is added in XCO version 3.8.2 to avoid this issue.
- Incremental downgrade to TPVM 4.7.10 will fail due to unsupported packages in TPVM 4.7.10. All other downgrade paths will succeed.

Unsupported characters in TPVM passwords

The following characters are not supported in TPVM passwords.

- & (ampersand)
- ! (exclamation mark)
- \ (backslash)
- ‘ (single quote)

Upgrading TPVM to 4.7.22

- Full Install is supported from version lower than 4.7.0
- Incremental upgrade is supported from version 4.7.0
- Minimum version requirements:
    - SLX-OS 20.6.3a
- Upgrade procedure
    - Step 1: Upgrade SLX-OS current version to SLX-OS 20.6.3a or above.
    - Step 2: Full upgrade TPVM to 4.7.22 if the current running TPVM version is lower than 4.7.0.

TPVM package list

The contents of the TPVM package list are available under the TPVM release folder on the Support Portal (in the form of a JSON file). The JSON file can be found here:

Below is a sample of the JSON file:


```
{
   "product": “TPVM”,
   "version": “4.7.22”,
   "packages": [
      {
        "package": "accountsservice",
```

```
        "version": "0.6.45-1ubuntu1.3",
        "architecture": "amd64",
        "description": "query and manipulate user account information"}
      },
```


……

tpvm_sec_upgrade.sh script

The 'tpvm_upgrade.sh' script is deprecated. Since Ubuntu's LTS version has been upgraded, it is necessary to perform a full upgrade.

This script cannot be used to upgrade to TPVM 4.7.22.