June 2026

Extreme TPVM 4.7.17

Release Notes

Supporting Extreme Routing and Extreme Switching SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150, Extreme 8820, Extreme 8720, and Extreme 8520

9039146-17 Rev AA

Contents

Document History

Version	Summary of changes	Publication date
REV AA	Initial version for 4.7.17	June 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 4.7.17 provides updated Hardening Script.

Security Update

- Security updates are included up to May 31st, 2026.

New Features

- The hardening script is updated to the latest version 0.97.13 and includes the blacklist script version 1.0.0. The blacklist script can be found within the `/opt/security/` directory along with the hardening script.

Common Vulnerabilities and Exposures (CVEs) Addressed in this release

The following CVEs are addressed in this release:

CVE	Module
CVE-2026-3039 CVE-2026-3592 CVE-2026-5946 CVE-2026-5950 (USN-8293-1)	bind9-dnsutils, bind9-host, bind9-libs
CVE-2026-4873 CVE-2026-5545 CVE-2026-5773 CVE-2026-6253 CVE-2026-6276 CVE-2026-6429 CVE-2026-7168 (USN-8227-1)	curl, libcurl3-gnutls, libcurl4
CVE-2026-4424 CVE-2026-4426 CVE-2026-5121 (USN-8292-1)	libarchive13
CVE-2026-24401 CVE-2026-34933 (USN-8269-1)	libavahi-client3, libavahi-common-data, libavahi-common3
CVE-2026-41989 (USN-8319-1)	libgcrypt20
CVE-2026-33845 CVE-2026-33846 CVE-2026-3832 CVE-2026-3833 CVE-2026-42009 CVE-2026-42010 CVE-2026-42011 CVE-2026-42012	libgnutls30

CVE-2026-42013 CVE-2026-42014 CVE-2026-42015 CVE-2026-5260 (USN-8284-1)	
CVE-2026-27135 (USN-8233-1)	libnghttp2-14
CVE-2026-33416 CVE-2026-33636 CVE-2026-34757 (USN-8251-1)	libpng16-16
CVE-2026-3731 (USN-8093-1)	libsmbclient, libwbclient0, samba-libs
CVE-2026-31419 CVE-2026-31431 CVE-2026-31533 CVE-2026-31504 CVE-2026-43033 CVE-2026-43077 CVE-2026-43078 CVE-2026-23351 CVE-2026-23274 CVE-2024-50060 CVE-2024-35862 (USN-8279-1)	Linux Kernel
CVE-2026-43964 (USN-8253-1)	postfix
CVE-2025-10158 CVE-2026-29518 CVE-2026-41035 CVE-2026-43617 CVE-2026-43618 CVE-2026-43619 CVE-2026-43620 (USN-8283-1)	rsync
CVE-2026-5958 (USN-8229-1)	sed
CVE-2026-3888 (USN-8102-1)	snapd
CVE-2026-42307 CVE-2026-44656 CVE-2026-45130 (USN-8304-1)	vim-common, vim-gtk3, vim-gui-common, vim-runtime, vim-tiny, vim, xxd

Changes in Behavior

The following are the behavioral changes made to HS v0.97.13 in TPVM 4.7.17 release.

- None

Hardware and Software Support

- TPVM 4.7.17 supports the following hardware platforms: SLX 9150, SLX 9250, SLX 9540, SLX 9640, SLX 9740, Extreme 8520, Extreme 8720, and Extreme 8820.
- Minimum supported SLX-OS version for TPVM 4.7.17 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 4.7.17.
  Note: Releases prior to TPVM 4.6.18 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 4.7.17.
    - Example: Incremental upgrade and downgrade between TPVM 4.6.16 and 4.7.17 versions is not supported. If a user attempts it, 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.

Unsupported characters in TPVM passwords

The following characters are not supported in TPVM passwords.

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

Upgrading TPVM to 4.7.17

- 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 4.7.17 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": “4.7.17”,
   "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 4.7.17.