

Release Notes

Version 6.22.1

Release Date: November 25, 2026

What's New in Version 6.22.1

The Securonix team is pleased to announce the availability of ThreatQ version 6.22.1. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

ThreatQ Platform

The following is a list of bug fixes and security updates for the ThreatQ platform included when you upgrade to 6.22.1.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.22.1.

- **Improved Upgrade Reliability and Performance:** Resolved several issues affecting the ThreatQ v6.22.0 upgrade process that could result in extended downtime, incomplete database migrations, or upgrade failures, particularly in environments with large datasets. These improvements enhance database migration reliability, reduce service interruptions during upgrades, and improve overall upgrade stability.
- **Resolved Web Interface Access Issue:** Fixed an issue introduced in ThreatQ v6.22.0 where accessing the ThreatQ web interface using an IP address resulted in a 404 Not Found error, while access through the fully qualified domain name (FQDN) continued to function normally. This update restores IP-based access for affected on-premises deployments while maintaining existing security and authentication requirements.
- **Improved Universal CSV Parser Stability:** Fixed an issue in the Universal CSV Parser Action where processing CSV files containing multiline quoted fields could cause excessive memory consumption, resulting in stalled workflows, service disruptions, or platform unavailability. The parser now correctly handles multiline CSV records, improving data ingestion reliability and preventing associated performance and stability issues.

Security and System Updates

The following updates have been made with ThreatQ v6.22.1:

- **Java4Shell (CVE-2026-114938) Security Mitigation:** Implemented recommended security measures to address the recently disclosed Java4Shell vulnerability (CVE-2026-114938) in the components used by ThreatQ v6 on-premises

deployments. These measures disable affected Java runtime methods to mitigate potential security risks while maintaining normal platform operations.

- **PHP Security Updates:** Updated the PHP components used by the ThreatQ platform to address recently disclosed security vulnerabilities. These updates incorporate security patches and improvements to mitigate potential risks and strengthen overall platform security.

  The following vulnerabilities were addressed as part of this update:

  - CVE-2026-115560
  - CVE-2026-126714
  - CVE-2026-129496
  - CVE-2026-129538
  - CVE-2026-129291
  - CVE-2026-129289
  - CVE-2026-129292
  - CVE-2026-128090
  - CVE-2026-15353
  - CVE-2026-129506
  - CVE-2026-128064
  - CVE-2026-127960

  The following vulnerabilities were also evaluated and determined not to affect the ThreatQ platform, based on the PHP versions and component configurations in use:

  - CVE-2026-129438
  - CVE-2026-48841
  - CVE-2026-129501
  - CVE-2026-129481
  - CVE-2026-129474
  - CVE-2026-129182

Upgrading

Perform the following steps to upgrade your ThreatQ v6 instance.

> ⚠ After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

1. Perform a platform check to ensure adequate disk space and that your installed integrations are compatible with the new ThreatQ version. You will be unable to proceed with the upgrade until clearing this check. It is important to note that the command does not apply to integrations installed on third-party systems such as the ThreatQ App for QRadar.

   Platform Check Against the Most Recent ThreatQ Version

   ```
   # sudo /usr/local/bin/tqadmin platform check
   ```

   Platform Check Against a Specific ThreatQ Version

   ```
   # sudo /usr/local/bin/tqadmin platform check -v 6.22.1
   ```

2. Run the upgrade command:

   Upgrade to the Latest ThreatQ Version

   ```
   # sudo /usr/local/bin/tqadmin platform upgrade
   ```

   Upgrade to a Specific ThreatQ Version

   ```
   # sudo /usr/local/bin/tqadmin platform upgrade -v 6.22.1
   ```

New Installations

If you are installing ThreatQ version 6 for the first time, it is highly recommended that you review the ThreatQ 6x Installation section and guides before proceeding with installation. The guide provides useful information including:

- Required Firewall Ports
- Suggested Partitioning Scheme
- System Requirements (Hardware Specifications, Core CPUs, RAM etc.)
- Steps to pin your RHEL 9 and Ubuntu versions to prevent upgrades to unsupported environments
- Security Hardening Guides

Migrating ThreatQ v5 to v6

It is important that you use the correct ThreatQ version when migrating a ThreatQ v5 instance to ThreatQ v6.

- Migrating to **ThreatQ v6.9.1 or greater** requires a **ThreatQ v5.29.5** backup file.
- Migrating to **ThreatQ v6.9.0** and prior requires a **ThreatQ v5.29.4** backup file.

⚠ Using a backup other than the ones listed above will result in a restore error.

Contact Securonix Support or your Technical Account Manager for additional information and to obtain the ThreatQ Migration Guide. The Securonix team highly recommends that you review the ThreatQ 6x Installation guide when planning your migration.

Support

Don't hesitate to get in touch with your Technical Account Manager to discuss planning your upgrade.

As always, contact our Customer Support Team if you encounter problems when upgrading or need assistance.

Thank you,

The Securonix Team

tq-support@securonix.com
ts.securonix.com
703.574.9893