Release Notes

Version 5.29.5

Released Date: June 11, 2025

What's New in Version 5.29.5

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.29.5. Below is a list of important bugs that have been addressed and upgrade instructions.

You can access these release notes, along with other ThreatQ product documentation on the ThreatQ Help Center.

Upgrade Impact

The upgrade is expected to take the standard amount of time for a ThreatQ upgrade. The exact time to complete the upgrade depends on your specific environment and resources.

Upgrading from...	Full Index Required	Data Migration Required	Server Reboot Required
5x (most recent version)	✗	✓	✓

ThreatQ Platform (TQ)

The following is a list of bug fixes for the ThreatQ platform.

NOTABLE BUG FIXES

- When a user with multi-factor authentication (MFA) enabled selects the Remember this computer for 30 days option at login, ThreatQ will not prompt the user for MFA for thirty days when using the current browser.

  > When you upgrade to this release, ThreatQ clears all existing Remember this computer for 30 days requests and requires each user to use MFA and reselect the option if applicable/desired.

- When ThreatQ attempted to ingest a STIX 1.2 file that included an ssdeep indicator, ThreatQ returned a namespace error. This occurred because the object namespace and rules were not loaded into the namespace definitions when an object type was previously found. We resolved this issue by updating STIX parsing to load base object information after a specific object type's information has been loaded.

Security and System Updates

The following Security updates have been made:

- Pynoceros:

UPDATED TO	CESA/GITHUB/OSV REF
certifi 2024.2.2	OSV PYSEC-2024-230 CVE-2024-39689 GHSA-248v-346w-9cwc
cryptography 42.0.4	GHSA-h4gh-qq45-vh27 GHSA-79v4-65xg-pq4g
idna 3.6	PYSEC-2024-60 CVE-2024-3651 GHSA-jjg7-2v4v-x38h
Jinja2 3.1.6	GHSA-q2x7-8rv6-6q7h GHSA-gmj6-6f8f-6699 GHSA-h75v-3vvj-5mfj GHSA-cpwx-vrp4-4pq7
PyMySQL 1.1.0	GHSA-v9hf-5j83-6xpp
requests 2.32.3	GHSA-9wx4-h78v-vm56
setuptools 80.9.0	GHSA-cx63-2mw6-8hw5 GHSA-5rjg-fvgr-3xxf
urllib3 2.4.0	GHSA-34jh-p97f-mpxf
zipp 3.21.0	GHSA-jfmj-5v4g-763

- Pynoceros messenger:

UPDATED TO	GITHUB REF
aiohttp 3.12.7	GHSA-jwhx-xcg6-8xhj GHSA-8495-4g3g-x7pr
cryptography 45.0.3	GHSA-h4gh-qq45-vh27 GHSA-79v4-65xg-pq4g
jinja2 3.1.6	GHSA-q2x7-8rv6-6q7h GHSA-gmj6-6f8f-6699 GHSA-cpwx-vrp4-4pq7
setuptools 80.9.0	GHSA-cx63-2mw6-8hw5 GHSA-5rjg-fvgr-3xxf

- Remote CentOS Linux 7 host:

UPDATED TO	CESA/RHSA REF		
Apache Solr 8.11.4	CVE-2015-1832	CVE-2020-36187	CVE-2024-29131
	CVE-2017-15095	CVE-2020-36188	CVE-2024-29133
	CVE-2017-17485	CVE-2020-36189	CVE-2024-2961
	CVE-2017-7525	CVE-2020-36518	CVE-2024-29857
	CVE-2018-11307	CVE-2020-8840	CVE-2024-30171
	CVE-2018-12022	CVE-2020-8908	CVE-2024-33599
	CVE-2018-1313	CVE-2020-9547	CVE-2024-33600
	CVE-2018-14718	CVE-2020-9548	CVE-2024-33601
	CVE-2018-14719	CVE-2021-20190	CVE-2024-33602
	CVE-2018-19362	CVE-2021-22569	CVE-2024-3596
	CVE-2018-5968	CVE-2022-3171	CVE-2024-37370
	CVE-2018-7489	CVE-2022-3509	CVE-2024-37371
	CVE-2019-12086	CVE-2022-3510	CVE-2024-38428
	CVE-2019-12384	CVE-2022-42003	CVE-2024-45490
	CVE-2019-12814	CVE-2022-42004	CVE-2024-45491
	CVE-2019-14379	CVE-2022-46337	CVE-2024-45492
	CVE-2019-14439	CVE-2023-31582	CVE-2024-4741
	CVE-2019-14540	CVE-2023-33202	CVE-2024-47535
	CVE-2019-14892	CVE-2023-44981	CVE-2024-47554
	CVE-2019-16335	CVE-2023-51074	CVE-2024-50602
	CVE-2019-16942	CVE-2023-51775	CVE-2024-52012
	CVE-2019-16943	CVE-2024-11053	CVE-2024-5535
	CVE-2019-17267	CVE-2024-12133	CVE-2024-6763

UPDATED TO	CESA/RHSA REF		
	CVE-2019-17531	CVE-2024-12243	CVE-2024-7254
	CVE-2019-20330	CVE-2024-13009	CVE-2024-7264
	CVE-2020-10650	CVE-2024-13176	CVE-2024-8096
	CVE-2020-10673	CVE-2024-21742	CVE-2024-8184
	CVE-2020-24616	CVE-2024-22201	CVE-2024-9143
	CVE-2020-24750	CVE-2024-23454	CVE-2024-9823
	CVE-2020-35490	CVE-2024-23944	CVE-2025-0395
	CVE-2020-35491	CVE-2024-2398	CVE-2025-24528
	CVE-2020-35728	CVE-2024-2511	CVE-2025-24814
	CVE-2020-36179	CVE-2024-25710	CVE-2025-24970
	CVE-2020-36180	CVE-2024-26308	CVE-2025-25193
	CVE-2020-36181	CVE-2024-26458	CVE-2025-27363
	CVE-2020-36182	CVE-2024-26461	CVE-2025-30258
	CVE-2020-36183	CVE-2024-28085	CVE-2025-31672
	CVE-2020-36184	CVE-2024-28182	CVE-2025-3576
	CVE-2020-36185	CVE-2024-28834	CVE-2025-4802
	CVE-2020-36186		
Apache Tika 3.1.0	CVE-2024-12133	CVE-2024-2511	CVE-2025-0395
	CVE-2024-12243	CVE-2024-33599	CVE-2025-0395
	CVE-2024-13009	CVE-2024-33600	CVE-2025-1390
	CVE-2024-13176	CVE-2024-33601	CVE-2025-21502
	CVE-2024-21131	CVE-2024-33602	CVE-2025-21587
	CVE-2024-21138	CVE-2024-4603	CVE-2025-29087
	CVE-2024-21140	CVE-2024-4741	CVE-2025-29088
	CVE-2024-21145	CVE-2024-5535	CVE-2025-30258
	CVE-2024-21147	CVE-2024-56406	CVE-2025-30691
	CVE-2024-21208	CVE-2024-6119	CVE-2025-30698
	CVE-2024-21210	CVE-2024-8184	CVE-2025-31115
	CVE-2024-21217	CVE-2024-9143	CVE-2025-3277
	CVE-2024-21235		

UPDATED TO	CESA/RHSA REF		
Apache Zookeeper 3.9.3	CVE-2022-3715 CVE-2022-40735 CVE-2022-46908 CVE-2023-2953 CVE-2023-4641 CVE-2023-48795 CVE-2023-52425 CVE-2023-5678 CVE-2023-6004 CVE-2023-6129 CVE-2023-6237 CVE-2023-6918 CVE-2023-7104 CVE-2024-0553 CVE-2024-0567 CVE-2024-0727 CVE-2024-11053 CVE-2024-12133 CVE-2024-12243 CVE-2024-12798 CVE-2024-12801 CVE-2024-13009 CVE-2024-13176 CVE-2024-22365	CVE-2024-23944 CVE-2024-2398 CVE-2024-2511 CVE-2024-26458 CVE-2024-26461 CVE-2024-28085 CVE-2024-28182 CVE-2024-28757 CVE-2024-28834 CVE-2024-28835 CVE-2024-2961 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-3596 CVE-2024-37370 CVE-2024-37371 CVE-2024-38428 CVE-2024-45490 CVE-2024-45491 CVE-2024-45492 CVE-2024-4603	CVE-2024-4741 CVE-2024-47535 CVE-2024-47554 CVE-2024-50602 CVE-2024-5535 CVE-2024-56406 CVE-2024-6119 CVE-2024-6763 CVE-2024-7264 CVE-2024-8096 CVE-2024-8176 CVE-2024-9143 CVE-2024-9681 CVE-2025-0395 CVE-2025-1390 CVE-2025-24528 CVE-2025-24970 CVE-2025-25193 CVE-2025-27363 CVE-2025-29088 CVE-2025-30258 CVE-2025-3576 CVE-2025-4802
dhclient 4.2.5	CVE-2023-4408		
httpd 2.4.6	RHSA-2024:4943		
kernel 3.10.0	RHSA-2024:5259		
krb5 1.15.1	RHSA-2024:5076		
libndp 1.2	RHSA-2024:4622		

UPDATED TO	CESA/RHSA REF		
MongoDB 7.0.21	CVE-2022-3715	CVE-2024-3596	CVE-2022-30634
	CVE-2024-28085	CVE-2024-37370	CVE-2022-30635
	CVE-2025-30258	CVE-2024-37371	CVE-2022-32189
	CVE-2024-28085	CVE-2025-24528	CVE-2022-41715
	CVE-2024-2961	CVE-2025-3576	CVE-2022-41716
	CVE-2024-33599	CVE-2024-26458	CVE-2022-41720
	CVE-2024-33600	CVE-2024-26461	CVE-2022-41722
	CVE-2024-33601	CVE-2024-28085	CVE-2022-41723
	CVE-2024-33602	CVE-2024-28182	CVE-2022-41724
	CVE-2025-0395	CVE-2024-28085	CVE-2022-41725
	CVE-2025-4802	CVE-2022-40735	CVE-2023-24534
	CVE-2024-2961	CVE-2024-6119	CVE-2023-24536
	CVE-2024-33599	CVE-2024-13176	CVE-2023-24537
	CVE-2024-33600	CVE-2024-2511	CVE-2023-24539
	CVE-2024-33601	CVE-2024-4603	CVE-2023-29400
	CVE-2024-33602	CVE-2024-4741	CVE-2023-29403
	CVE-2025-0395	CVE-2024-5535	CVE-2023-39325
	CVE-2025-4802	CVE-2024-9143	CVE-2023-45283
	CVE-2025-1390	CVE-2024-12133	CVE-2023-45287
	CVE-2024-2398	CVE-2024-28085	CVE-2023-45288
	CVE-2024-7264	CVE-2023-4641	CVE-2024-34156
	CVE-2024-8096	CVE-2024-28085	CVE-2022-1705
	CVE-2024-11053	CVE-2022-40735	CVE-2022-1962
	CVE-2024-9681	CVE-2024-6119	CVE-2022-32148
	CVE-2024-12243	CVE-2024-13176	CVE-2022-41717
	CVE-2024-28834	CVE-2024-2511	CVE-2023-24532
	CVE-2024-28835	CVE-2024-4603	CVE-2023-29406
	CVE-2024-3596	CVE-2024-4741	CVE-2023-29409
	CVE-2024-37370	CVE-2024-5535	CVE-2023-39318
	CVE-2024-37371	CVE-2024-9143	CVE-2023-39319
	CVE-2025-24528	CVE-2023-4641	CVE-2023-39326
	CVE-2025-3576	CVE-2024-56406	CVE-2023-45284
	CVE-2024-26458	CVE-2024-28085	CVE-2023-45289
	CVE-2024-26461	CVE-2023-24538	CVE-2023-45290
	CVE-2024-3596	CVE-2023-24540	CVE-2024-24783
	CVE-2024-37371	CVE-2024-24790	CVE-2024-24784
	CVE-2025-24528	CVE-2022-27664	CVE-2024-24785
	CVE-2025-3576	CVE-2022-28131	CVE-2024-24789
	CVE-2024-26458	CVE-2022-2879	CVE-2024-24791
	CVE-2024-26461	CVE-2022-2880	CVE-2024-34155
	CVE-2024-3596	CVE-2022-29804	CVE-2024-34158
	CVE-2024-37370	CVE-2022-30580	CVE-2024-45336
	CVE-2024-37371	CVE-2022-30630	CVE-2024-45341

UPDATED TO	CESA/RHSA REF		
	CVE-2025-24528 CVE-2025-3576 CVE-2024-26458 CVE-2024-26461	CVE-2022-30631 CVE-2022-30632 CVE-2022-30633	CVE-2025-22866 CVE-2025-22871 CVE-2022-30629
nginx 1.27.5	CVE-2023-42366 CVE-2023-42363 CVE-2023-42364 CVE-2023-42365 CVE-2024-7347		
operations manager 5.29.5	GHSA-248v-346w-9cwc PYSEC-2024-230 GHSA-5rjg-fvgr-3xxf		
python-setuptools 0.9.8	RHSA-2024:6662		
websocket server 5.29.5	GHSA-8hc4-vh64-cxmj GHSA-jr5f-v2jv-69x6 GHSA-pxg6-pf52-xh8x GHSA-cxjh-pqwp-8mfp GHSA-3h5v-q93c-6h6q		

Install Notes

- To upgrade from a 4x version to versions 5.6 through 5.18, you must be on the most recent 4x release. To upgrade to 5.19 or later, you must first upgrade to release 5.13 or later.
- For the upgrade from the most recent 4x release to versions 5.6 through 5.18, you will need to enter your MariaDB root password during the upgrade process. To upgrade from 5.13 or later to 5.19 or later, you may need to enter your MariaDB root password during the upgrade process.
- The following warning will be displayed during the upgrade process:
  `Warning: RPMD altered outside of yum.`
  `**Found 5 pre-existing rpmdb problem(s), 'yum' check output follows`
  This warning does not require any action on your part and will be resolved during the upgrade.
- Do not restart your instance during the upgrade process.

We highly recommend that you perform a backup of your ThreatQ instance before upgrading.

How to Upgrade

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

Platform Check

ThreatQ version 5x provides you with the ability to run an independent preflight check, prior to upgrading, to ensure adequate disk space. The system will also scan your installed integrations for any incompatible versions. You will be unable to perform the upgrade if an incompatible integration version is detected.

This scan does not apply to integrations installed on third-party systems such as the ThreatQ App for QRadar.

Run a platform check for the most recent ThreatQ version:

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

Run a platform check for a specific version:

```
# sudo /usr/local/bin/tqadmin platform check -v <version number>
```

Upgrade Commands

To upgrade, run the following command:

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

To upgrade to a specific version, run the following command:

```
# sudo /usr/local/bin/tqadmin platform upgrade -v <version number>
```

To discuss planning your upgrade, do not hesitate to get in touch with your Customer Success Engineer.

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

Thank you,

The ThreatQuotient Team

support@threatq.com
support.threatq.com
703.574.9893