Cisco Tetration Release Notes Release 3.3.2.23

This document describes the features, caveats, and limitations for the Cisco Tetration software, release 3.3.2.23.

The Cisco Tetration platform is designed to comprehensively address a number of data center operational and security challenges using rich traffic telemetry collected from servers, layer 4 through 7 service elements, and end-point devices (such as laptops, desktops, and smartphones). The platform performs advanced analytics using an algorithmic approach to offer a holistic workload protection platform. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis. The platform provides a ready-to-use solution supporting the following use cases:

- Provide behavior-based application insight to automate allowed-list policy generation
- Provide application segmentation to enable efficient and secure zero-trust implementation
- Provide consistent policy enforcement across on-premises data centers, and private and public clouds
- Identify process behavior deviations, and software vulnerabilities and exposure to reduce attack surface
- Identify application behavior changes and policy compliance deviations in near-real time
- Support comprehensive telemetry processing in a heterogeneous environment to provide actionable insight within minutes
- Enable long-term data retention for deep forensics, analysis, and troubleshooting

To support the analysis and various use cases within the Cisco Tetration platform, consistent telemetry is required from across the data center infrastructure. Rich Cisco Tetration telemetry is collected using agents. There are different types of agents available to support both existing and new data center infrastructures. This release supports the following agent types:

- Software agents installed on virtual machine, bare-metal, or container hosts
- ERSPAN agents that can generate Cisco Tetration telemetry from copied packets
- Telemetry ingest from ADCs (Application Delivery Controllers) – F5, Citrix and AVI
- NetFlow agents that can generate Cisco Tetration telemetry based on NetFlow v9 or IPFIX records
- Embedded hardware agents in Cisco Nexus 9000 CloudScale series switches

In addition, this release supports ingesting endpoint device posture, context and telemetry through integrations with:

- Cisco AnyConnect installed on endpoint devices such as laptops, desktops, and smartphones
- Cisco ISE (Identity Services Engine)

Software agents also act as the policy enforcement point for the application segmentation. Using this approach, the Cisco Tetration platform enables consistent microsegmentation across public, private, and on-premises deployments. Agents enforce the policy using native operating system capabilities, thereby eliminating the need for the agent to be in the data path and providing a fail-safe option. Additional product documentation is listed in the “Related Documentation” section.

These Release Notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html

The following table shows the online change history for this document.

Table 1 Online History Change

Date	Description
March 16th, 2020	Release 3.3.2.23 became available.

Contents

This document includes the following sections:

New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

New Software Features

No new software features in this patch release.

Changes in Behavior

These are changes in behavior for this release:

- Scope query evaluation is case-insensitive. Consider a case where inventory a.b.c.d is assigned a Tag *Environment = Dev. If we define a scope with query *Environment == DEV we will ensure that this new scope will have inventory a.b.c.d as its member.
- Side Channel attack detection for Anomalous cache activity has been restored. Please note this feature remains experimental.
- The Threat Intelligence feature no longer requires adding s3.us-west-1.amazonaws.com and s3.us-west-2.amazonaws.com to the Allow-list. Note that threat datasets will be served by uas.tetrationcloud.com, so adding uas.tetrationcloud.com to the Allow-list is still required.

- The External Orchestrator plugin for Infoblox now uses a less strict method to probe for supported WAPI versions of the specified Infoblox appliance, as the former code requires WAPI version 2.7.1 to start with. With this release WAPI 2.6, 2.6.1, 2.7 and 2.7.1 (the recommended version) are supported.
- An Activation Key is added to the agent download page; this enables users to register agents under different root scopes without having to add VRF configuration rules. An Activation Key is optional for new sensor installs; that is, old installer scripts will continue to work. If the installer script contains an Activation Key, it will aid placing the sensor in the correct root scope (no need for any agent intents). If an Activation Key is not present, the sensor will land in the default root scope (old behavior), and agent intents will be needed to move it to a different scope.
- The “Test HTTP Proxy” button on the Company -> Outbound HTTP page will be active only after proxy information is saved successfully, since the proxy port number needs to be allowed in the Tetration Cluster first.
- The Scopes page now shows the updated query (vs. the current query) before scope updates have been committed.

Enhancements

- Tetration gathers information about Windows security patches applied on the workload and uses that information along with a feed from Microsoft to filter out CVEs fixed by those patches.
- Tetration uses information delivered through a Redhat Security Data feed to match and report CVEs against installed package versions.
- There is a new ‘Auto accept outgoing policy connector’ option in Default ADM Run configuration which applies to the root scope. Enabling this option auto-accepts policy connectors in the applications within that root scope without you having to accept them or add auto-accept rules for them.
- A new snapshot command ‘tnp_datastream’ is added to allow customer support personnel to create a snapshot file with policy stream data processed by Load Balancer enforcement agents. This is needed for post debugging of issues related to Load Balancer enforcement agents.
- A table with supported versions for external orchestrators is added to the user guide, section Inventory - User Annotations.
- A ‘Deep Policy Generation’ mode for ADM Run. Enabling ‘Deep Policy Generation’ directs ADM to discover Allow-list policies for all the endpoints under the current workspace scope and all its offspring scopes. Such an ADM run skips clustering and suggests all policies based on scopes. This mode is available for all scopes.
- Policy quick-analysis works with unknown IP addresses that are not traced in the Tetration system. Unknown IP addresses will be treated as a root scope or an Internet endpoint during quick-analysis, and policies will be matched accordingly.
- If a hardware failure is detected upon restart of a cluster after a power shut-down, currently the system is stuck in a situation where neither a Reboot workflow can be run to get services stable, nor can a Commission workflow be run, as down services result in a commissioning failure. The new “bmexclude” feature will help alleviate such situations by allowing you to reboot (upgrade) with bad hardware, after which the regular RMA process for the failed bare-metal can be performed.
- The Applications tab/section has been renamed to Segmentation. Filter (Scope, Inventory Filter and Cluster) label styles have been updated.
- When creating or deleting a scope, the parent will only be marked dirty if a commit scope updates action is necessary. It is possible to create and delete scopes without the action becoming visible.
- An Activation Key is added to the agent download page; this enables users to register agents under different root scopes without having to add NAT rules. This Activation Key is optional for new sensor installs (that is, old installer

scripts will continue to work). If the installer script contains an Activation Key, that will help land the sensor in the correct root scope (no need for any agent intents). If an Activation Key is not present, the sensor will land in the Default root scope (old behavior) and agent intents will be needed to move it to a different scope.

Caveats

This section contains lists of open and resolved caveats, as well as known behaviors.

Open Caveats

No new open caveats.

Resolved Caveats

The following table lists the resolved caveats in this release. Click a bug ID to access Cisco's Bug Search Tool to see additional information about that bug.

Table 3 Resolved Caveats

Bug ID	Description
CSCvs62653	CVE-2018-15514 vulnerability in Docker for Windows is detected on a Linux system
CSCvs76207	Scope definition using tags have a mixed case sensitive / insensitive behavior
CSCvt04418	Compliance alerts in Kafka will have an additional field "alert_details_json" with proper json matching "alert_details".
CSCvt06117	There will be a new type of compliance alert that can be used to alert on flows matching a catch-all policy rule.
CSCvs51469	In some cases, during Tetration boot up (after power down) UI prevents login with bad gateway error
CSCvq78961	Policy quick analysis works with unknown IP addresses that are not traced in the Tetration system.
CSCvt21055	AIX 7.1 agent is unable to connect to Tetration cluster when strong ciphers are enabled.
CSCvt08560	Tetration AIX agent may use bpf interfaces which conflict with other system devices
CSCvt06585	Unable to see TCP retransmits stats from the Windows agents. In the fix, agents invoke Win32 API to get the number of retransmitted bytes and estimate the number of retransmitted packets.
CSCvr61273	Unable to test HTTP Proxy after clicking Save button
CSCvr80681	ADM AppView conversations are not getting properly displayed
CSCvs35823	External Orchestrator - change "Insecure" checkbox to "accept self-signed cert"

Known Behaviors

- During upgrade when a new RPM is uploaded, adhocKafka is gracefully shut down. This is done to avoid Kafka index corruption. Kafka comes back up after the upgrade. If upgrade is aborted after uploading the RPM, adhocKafka should be restarted using the explore command.
- After upgrading to 3.3.2.23, any Tetration external appliances (Tetration Ingest, Tetration Edge, or Tetration Export) that are behind a proxy need to be rebooted. This will reconnect with the Tetration cluster and register the appliance and connectors successfully.

Compatibility Information

The software agents in the 3.3.2.23 release support the following operating systems (virtual machines and bare-metal servers) for microsegmentation (deep visibility and enforcement):

- Linux:
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.7
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.7
  - Redhat Enterprise Linux-8.0
  - Oracle Linux Server-6.x: 6.1 to 6.10
  - Oracle Linux Server-7x: 7.0 to 7.7
  - SUSE Linux-11.x: 11.2, 11.3, and 11.4
  - SUSE Linux-12.x: 12.0, 12.1, 12.2,12.3, 12.4
  - SUSE Linux-15.x: 15.0, 15.1
  - Ubuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04
- Windows Server (64-bit):
  - Windows Server 2008R2 Datacenter
  - Windows Server 2008R2 Enterprise
  - Windows Server 2008R2 Essentials
  - Windows Server 2008R2 Standard
  - Windows Server 2012 Datacenter
  - Windows Server 2012 Enterprise
  - Windows Server 2012 Essentials
  - Windows Server 2012 Standard
  - Windows Server 2012R2 Datacenter
  - Windows Server 2012R2 Enterprise
  - Windows Server 2012R2 Essentials
  - Windows Server 2012R2 Standard
  - Windows Server 2016 Standard
  - Windows Server 2016 Essentials
  - Windows Server 2016 Datacenter

  - Windows Server 2019 Standard
  - Windows Server 2019 Essentials
  - Windows Server 2019 Datacenter
- Windows VDI desktop Client:
  - Microsoft Windows 8
  - Microsoft Windows 8 Pro
  - Microsoft Windows 8 Enterprise
  - Microsoft Windows 8.1
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Enterprise
  - Microsoft Windows 10
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 Enterprise 2016 LTSB
- IBM AIX operating system (Alpha):
  - AIX version 7.1
  - AIX version 7.2
- Container host OS version for policy enforcement:
  - Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4, 7.7
  - CentOS Release 7.1, 7.2, 7.3, 7.4, 7.7
  - Ubuntu-16.04

The 3.3.2.23 release supports the following operating systems for visibility use cases only:

- Linux:
  - CentOS-5.x: 5.7 to 5.11
  - Redhat Enterprise Linux-5.x: 5.7 to 5.11
- Windows Server (64-bit):
  - Windows Server 2008 Datacenter
  - Windows Server 2008 Enterprise
  - Windows Server 2008 Essentials
  - Windows Server 2008 Standard
- Windows VDI desktop Client:
  - Microsoft Windows 7
  - Microsoft Windows 7 Pro
  - Microsoft Windows 7 Enterprise

The 3.3.2.23 release supports the following operating systems for the universal visibility agent:

- Redhat Enterprise Linux 4.0 (32-bit and 64-bit)
- CentOS 4.0 (32-bit and 64-bit)
- Redhat Enterprise Linux 5.0 (32-bit)
- CentOS 5.0 (32-bit)
- Windows Server (32-bit and 64-bit)
- Solaris 11 on x86 (64-bit)
- AIX 5.3 (PPC)

The 3.3.2.23 release supports the following Cisco Nexus 9000 series switches in NX-OS and Cisco Application Centric Infrastructure (ACI) mode:

Table 4 Supported Cisco Nexus 9000 Series Switches in NX-OS and ACI Mode

Product line	Platform	Minimum Software release
Cisco Nexus 9300 platform switches (NX-OS mode)	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco NX-OS Release 9.2.1 and later
	Cisco Nexus 93180YC-FX, 93108TC-FX, and 9348GC-FXP	Cisco NX-OS Release 9.2.1 and later
	Cisco Nexus 9336C-FX2	Cisco NX-OS Release 9.2.1 and later
Cisco Nexus 9300 platform switches (ACI mode)	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 93180YC-FX, 93108TC-FX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9348GC-FXP	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9336C-FX2	Cisco ACI Release 3.2 and later
	Cisco Nexus 9500 series switches with N9K-X9736C-FX linecards only	Cisco ACI Release 3.1(1i) and later

Usage Guidelines

This section lists usage guidelines for the Cisco Tetration Analytics software.

- You must use the Google Chrome browser version 40.0.0 or later to access the web-based user interface.
- After setting up your DNS, browse to the URL of your Cisco Tetration Analytics cluster: https://<cluster.domain>

Verified Scalability Limits

The following tables provide the scalability limits for Cisco Tetration (39-RU), Cisco Tetration-M (8-RU), and Cisco Tetration Cloud:

Table 5 Scalability Limits for Cisco Tetration (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or Baremetal)
Flow features per second	Up to 2 Million
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 6 Scalability Limits for Cisco Tetration-M (8-RU)

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or Baremetal)
Flow features per second	Up to 500,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 7 Scalability Limits for Cisco Tetration Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or bare-metal)
Flow features per second	Up to 70,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Not supported

Note: Supported scale will always be based on which ever parameter reaches the limit first.

Related Documentation

The Cisco Tetration Analytics documentation can be accessed from the following websites:

Tetration Datasheets: https://www.cisco.com/c/en/us/products/security/tetration/datasheet-listing.html

General Documentation: https://www.cisco.com/c/en/us/support/security/tetration/tsd-products-support-series-home.html

The documentation includes installation information and release notes.

Table 8 Installation Documentation

Document	Description
Cisco Tetration Analytics Cluster Deployment Guide	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Tetration (39-RU) platform and Cisco Tetration-M (8-RU). Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html
Cisco Tetration Virtual Deployment Guide	Describes the deployment of Tetration virtual appliance. Document Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html
Cisco Tetration Cluster Upgrade Guide	Documentation Link: https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Upgrade_Guide.html
Latest Threat Data Sources	https://updates.tetrationcloud.com/