Cisco Tetration Release Notes Release 3.3.2.50

This document describes the features, caveats, and limitations for the Cisco Tetration software, release 3.3.2.50.

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 allow-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-deployment and new-deployment 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 ingestion 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, support is provided for 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 application segmentation. Using this approach, the Cisco Tetration platform enables consistent micro segmentation 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.

Date	Description
September 11th, 2020	Release 3.3.2.50 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

Software agent support added for Redhat Enterprise Linux 8.2, CentOS 8.0 and CentOS 8.1 to support all workload protection capabilities.

Changes in Behavior

- No changes in behavior for this patch

Enhancements

- Some of the UCS M4-based Tetration 39RU clusters may contain Solid State Drives (SSDs) in the TA-SNODE-G1 nodes that are impacted by the field notice - https://www.cisco.com/c/en/us/support/docs/field-notices/705/fn70545.html. In this patch, there is an explore endpoint (fieldnotice_7545) that will report and remediate this issue.
- Please use a POST to orchestrator.service.consul with a snapshot path of fieldnotice_7545?usage=true to get details on how to use this endpoint. The endpoint runs in the background and will return a report in two to three minutes that indicates which drives are potentially affected and how many hours they have been in operation.

- To view the details of the report please POST to orchestrator.service.consul with a snapshot path of: cat?args=/local/logs/tetration/snapshot/cmdlogs/snapshot_fieldnotice_7545_log.txt. The cat endpoint may not return any data until the command is completed.
- When the explore endpoint is run as fieldnotice_7545?args=-fix the endpoint will apply the SSD firmware upgrade to remediate the issue; the entire process usually takes approximately 15 minutes to complete. Drives are updated one at a time so there should be minimal to no impact to services. Since this process runs in the background it requires the cat command to view the output.

Caveats

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

Open Caveats

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

Bug ID	Description
CSCvv09685	The Tetration enforcement (EFE) traffic on port 5660 is not filtered out and will be shown in policy analysis. If there are no corresponding policies to allow this traffic, the flows will show up as ESCAPED in policy analysis and enforcement analysis and may trigger alerts. A workaround is to create manual ALLOW policies to cover this traffic.

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.

Bug ID	Description
CSCvu95948	Sensor workload profile vulnerabilities tab does not permit to filter on Package Version
CSCvt91592	Multicast flows are excluded from policy analysis within an application workspace.
CSCvv28548	RHEL/CentOS 5.x sensor incorrectly rejects new 3.4 forensics rules due to incorrect sanitization
CSCvv32791	F5 having 13.X.X version not able to integrate into Tetration as external orchestrator.
CSCvv13955	Agents installed packages checks may create multiple DismHost.exe files under C:\Windows\Temp

Known Behaviors

- No known behavior changes

Compatibility Information

The software agents in the 3.3.2.50 release support the following operating systems (virtual machines and bare-metal servers) for micro segmentation (deep visibility and enforcement):

- Linux:
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.7
  - CentOS-8.x: 8.0 to 8.1
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.8
  - Redhat Enterprise Linux-8.x: 8.0 to 8.2
  - 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, 12.5
  - 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 3.3.2.50 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 3.3.2.50 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 3.3.2.50 release supports the following Cisco Nexus 9000 series switches in NX-OS and Cisco Application Centric Infrastructure (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:

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or new deployment)
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

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or new deployment)
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

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or new deployment)
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	Document 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/