Cisco Tetration Release Notes Release 3.4.1.20

This document describes the features, bug fixes and any behavior changes for the Cisco Tetration software patch release 3.4.1.20. This patch is associated with the Tetration software major release 3.4.1.1. Details of the major release can be found here - https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/release-notes/cta_rn_3_4_1_1.html.

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
November 30th, 2020	Release 3.4.1.20 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 7.9, Ubuntu 20.04, CentOS 8.2 and Oracle Linux 8.2 to support all workload protection capabilities.
- In workload profile summary page where Tetration software agent is installed, user with right privileges will be able to download agent logs. This feature is available for all deep Visibility and enforcement Agents.

Changes in Behavior

Due to platform security enhancements to on-prem appliances in this release, access to OpenAPI and Web UI will be restricted to the fully qualified domain name (FQDN) as configured in Company -> Cluster Configuration. As a result, the following are expected behaviors:

- If existing UI FQDN contains upper-case characters, the FQDN will be converted to lower-case to match browser redirect handling
- Attempt to access UI/API via IP address will be redirected to the cluster FQDN. Prior to upgrading to this patch release, customers are advised to verify that the UI FQDN is resolved correctly in their DNS resolvers

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 2 to 3 minutes that indicates which drives are potentially impacted 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 completes.
  - 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.
- External Orchestrator F5 integration now supports reading health check configuration from F5 appliances. These health checks for the pool of members are referred to as *Monitors* in F5 terminology. The additional configuration is used by the enforcement engine to automatically permit health check traffic to backend members, making intents previously added for this purpose redundant.
- With this release, inventory annotation via DNS orchestrator has been enhanced to now annotate any matching inventory (learned or static), even if the IP is not explicitly learned through agent or inventory upload. This information will be displayed as a single multi-value annotation called “orchestrator_system/dns_name”, whose value will be the DNS entries that point (directly or indirectly) to that IP address.
- Enhancements to Admiral alerts:
  - Detect and alert on disk failure, DIMM (Memory) failure and Fan speed issues.
  - Disk usage warning and critical alerts enhanced to monitor /root, /tmp and /var/log.

- The product usage analytics feature has been added to help understand, improve and research services provided by Tetration. This telemetry collection adheres to Cisco Universal Cloud Agreement for SaaS (https://www.cisco.com/c/en/us/about/legal/cloud-and-software/universal-cloud-agreement.html) and Cisco End User License Agreement for on-premises deployments (https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html). Tetration users can opt-out of this usage data collection feature completely at Company -> Usage Analytics page and this does not impact any product functionality.

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.

Table 3 Open Caveats

Bug ID	Description
CSCvv62757	Download of CSV fails if user annotation column is multi-value.

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 4 Resolved Caveats

Bug ID	Description
CSCvv77377	Tetration Enforcement Deviation Enhancements
CSCvw03485	UCS HDD firmware update hangs on MTFDDAK3T8TDC solid state drives
CSCvw05529	Patch upgrade to 3.4.1.14 user login does not work if site_ui_fqdn has uppercase letters
CSCvv48981	CURL is replaced by sensortools.exe in 3.4 but CURL is in log output
CSCvv96201	Added srtt_dim_usec, fwd_tcp_bottleneck and rev_tcp_bottleneck as filter columns for openapi flowsearch.
CSCvu90994	Hardware agents (leaf switches) are not getting auto upgraded post patch upgrade

CSCvv40803	Agent installer does not check precise for openssl version
CSCvv81463	UCS firmware update does not upgrade disk firmware
CSCvv90370	AnyConnect Connector does not support AnyConnect 4.9 IPFIX templates.
CSCvw47120	Windows enforcer creates duplicate firewall rules when EFE is not reachable due to network issues
CSCvw48352	Workload resource contention with large policy may lead to duplicate Windows Firewall rules
CSCvw54456	Windows Enforcement Agent logs policy deviation detected error continuously

Known Behaviors

- 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.

Compatibility Information

The software agents in the 3.4.1.20 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 7.8
  - CentOS-8.x: 8.0 to 8.2
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.9
  - 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 7.8
  - Oracle Linux Server-8.x: 8.0 to 8.2
  - 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 and 12.5
  - SUSE Linux-15.x: 15.0, 15.1 and 15.2
  - Ubuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04
  - Ubuntu-20.04
- 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 (Beta):
  - 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 3.4.1.20 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

The 3.4.1.20 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 3.4.1.20 release supports the following Cisco Nexus 9000 series switches in NX-OS and Cisco Application Centric Infrastructure (ACI) mode:

Table 5 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 6 Scalability Limits for Cisco Tetration (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or bare-metal)
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 7 Scalability Limits for Cisco Tetration-M (8-RU)

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or bare-metal)
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 8 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	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/

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2020 Cisco Systems, Inc. All rights reserved.