ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Update 7

Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Update 7

Maintenance Report Number: CCEVS-VR-VID11417-2025

Date of Activity: 25 February 2025

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Trellix Intrusion Prevention System Sensor and Manager Appliances Impact Analysis Report For Common Criteria Assurance Maintenance
- Collaborative Protection Profile for Network Devices, Version 2.2e
- PP-Module for Intrusion Protection Systems (IPS), Version 1.0
- Vulnerability Assessment for Trellix Intrusion Prevention System Sensor and Manager Appliances v11.1 Update 7, Version 0.4, January 29th, 2024
- Equivalency Analysis for Trellix Intrusion Prevention System Sensor Appliances version 11.1 Update 7, Version 0.1, November 18, 2024

Original Documentation:

- Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target, Version 1.9, May 14, 2024
- Trellix Intrusion Prevention System 11.1.x Installation Guide
- Trellix Intrusion Prevention System 11.1.x Product Guide
- Trellix Intrusion Prevention System Manager Appliance Product Guide
- Trellix Intrusion Prevention System NS-series Sensor Product Guide
- Trellix Intrusion Prevention System 11.1 FIPS and CC Certification Guide

Revised Documentation:

- Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Update 7 Security Target, Version 2.0, November 2024
- Trellix Intrusion Prevention System 11.1.x Installation Guide, 11.1 Update 7, 28 Nov 2024
- Trellix Intrusion Prevention System 11.1.x Product Guide, 11.1 Update 7, 28 Nov 2024
- Trellix Intrusion Prevention System Manager Appliance Product Guide, 11.1 Update 7, 28 Nov 2024

- Trellix Intrusion Prevention System NS-series Sensor Product Guide, 11.1 Update 7, 28 Nov 2024
- Trellix Intrusion Prevention System 11.1 FIPS and CC Certification Guide, 11.1 Update 7, 28 Nov 2024
- Trellix Intrusion Prevention System NS3600 Sensor Hardware Guide, 11.1 Update 7, 28 Nov 2024
- Trellix Intrusion Prevention System NS7600 Sensor Hardware Guide, 11.1 Update 7, 28 Nov 2024
- Trellix Intrusion Prevention System NS9600 Sensor Hardware Guide, 11.1 Update 7, 28 Nov 2024

Assurance Continuity Maintenance Report:

Acumen Security submitted an Impact Analysis Report (IAR) for the Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 8 December 2024. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target, the CC Certification Guide, the Installation Guide, the Product Guides, the Hardware Guides and the Impact Analysis Report (IAR) (see above for a full list of documentation). The ST, Admin Guides, and IAR were updated.

The information below has all been pulled from the IAR, updated ST and updated AGDs provided for this assurance maintenance action.

Documentation updated:

Original CC Evaluation Evidence	**Evidence Change Summary**
Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target, Version 1.9, May 14, 2024	The ST has been revised to update the following: • Updated TOE version from 11.1 to 11.1 Update 7. • Addition of the new IPS-NS9600 Sensor to the claimed platforms and CAVP certificates (A3350 and A3353).
Design Documentation: See Security Target and Guidance	See Security Target and Guidance changes in this table

Guidance Documentation: Trellix Intrusion Prevention System 11.1.x Installation Guide Trellix Intrusion Prevention System 11.1.x Product Guide Trellix Intrusion Prevention System Manager Appliance Product Guide Trellix Intrusion Prevention System NS-series Sensor Product Guide Trellix Intrusion Prevention System 11.1 FIPS and CC Certification Guide	The AGDs have been revised to update the following: Trellix Intrusion Prevention System 11.1.x FIPS and CC Certification Guide • Incorporation of all new features and enhancements introduced across the Update 6 and Update 7 releases. • Updated mentions of Manager and Sensor versions from 11.1.19.3 and 11.1.17.2 to 11.1.19.46 and 11.1.17.46 respectively. • Inclusion of mention of the new IPS-NS9600 TOE platform. Trellix Intrusion Prevention System 11.1.x Installation Guide • Incorporation of all new features and enhancements introduced across the Update 6 and Update 7 releases. • Inclusion of mention of the new IPS-NS9600 TOE platform. Trellix Intrusion Prevention System Manager Appliance Product Guide • Incorporation of all new features and enhancements introduced across the Update 6 and Update 7 releases. • Updated mentions of Manager and Sensor versions from 11.1.19.3 and 11.1.17.2 to 11.1.19.46 and 11.1.17.46 respectively. • Inclusion of mention of the new IPS-NS9600 TOE platform. Trellix Intrusion Prevention System NS-series Sensor Product Guide • Incorporation of all new features and enhancements introduced across the Update 6 and Update 7 releases. • Updated mentions of Manager and Sensor versions from 11.1.19.3 and

	11.1.17.2 to 11.1.19.46 and 11.1.17.46 respectively. • Inclusion of mention of the new IPS-NS9600 TOE platform. Trellix Intrusion Prevention System 11.1.x Product Guide • Incorporation of all new features and enhancements introduced across the Update 6 and Update 7 releases. • Updated mentions of Manager and Sensor versions from 11.1.19.3 and 11.1.17.2 to 11.1.19.46 and 11.1.17.46 respectively. • Inclusion of mention of the new IPS-NS9600 TOE platform. Trellix Intrusion Prevention System NS3600 Sensor Hardware Guide • New hardware guidance document for the previously evaluated IPS-NS3600 Sensor platform. Trellix Intrusion Prevention System NS7600 Sensor Hardware Guide • New hardware guidance document for the previously evaluated IPS-NS7600 Sensor platform. Trellix Intrusion Prevention System NS9600 Sensor Hardware Guide • New hardware guidance document for the newly added IPS-NS9600 Sensor platform.
Lifecycle: None	No changes required.
Testing: None	No changes required. Release testing and certified image software testing are performed by the vendor against each release and/or software build to ensure that the TOE functionality is maintained and

	that the source code is fit for use. These include verification that any newly introduced features or enhancements do not affect the security functionality previously tested and verified. See below for more details.
Vulnerability Assessment: None	Acumen performed a search of public information for potential vulnerabilities on January 29, 2025. The search was in accordance with Labgram #116/Valgram #135 - Vulnerability Evidence. The vulnerability Assessment was reperformed for the TOE. The following documents the results of the updated assessment: • Vulnerability Assessment for Trellix Intrusion Prevention System Sensor and Manager Appliances v11.1 Update 7, version .4, January 29, 2025 See more details including search terms below.

Changes to the TOE:
The changes are summarized below.

Major Changes

None.

Minor Changes

Hardware Changes and Impact
Hardware Changes 11.1 Update 7:

Type of Change	Impact Analysis
New platform	**IPS-NS9600:** A new IPS-NS9600 Sensor model with the XEON GOLD 5520+ CPU is added to the scope. • **Impact: Minor** • **Rationale: The XEON GOLD 5520+ CPU used in the IPS-NS9600 Sensor is considered equivalent to the XEON SILVER 4416+ CPU used in the certified IPS-NS7600 Sensor. Hence, there is no relevant impact. Further details can be found in the Equivalency Analysis document.**

Software Changes and Impact:
Software Changes 11.1 Update 7:

Type of Change	Impact Analysis
New Features	**IPS-NS9600:** The 11.1 Update 7 Release introduces support for the new IPS-NS9600 Sensor model along with a new Sensor software image for the same. • **Impact: Minor** • **Rationale: The new IPS-NS9600 Sensor is considered equivalent to the certified IPS-NS7600 Sensor. Further details can be found in the Equivalency Analysis document. Moreover, added support for the new Sensor does not impact the rest of the Manager or Sensor functionalities. Hence, there is no relevant impact.**
Enhancements	**RSA 4096-bit key support:** The 11.1 Update 7 Release adds support for establishing the intra-TOE Sensor-Manager TLS channel using certificates with a 4096-bit RSA key. In earlier releases, this was restricted to only 2048-bit RSA. • **Impact: Minor** • **Rationale: Despite the added support for configurability of 4096-bit RSA, the default configuration across both Managers and Sensors is set to the evaluated 2048-bit RSA. Moreover, Section 'Managing Certificates for Manager and Sensor' of the 'Trellix Intrusion Prevention System 11.1.x Product Guide' includes a note stating that only 2048-bit RSA should be configured and used when the TOE is deployed in a CC configuration. Hence, it does not affect the evaluated TSF.** **DNS Response Fields' Support for Layer 7 Data Collection:** The Update 7 release builds upon the Update 6 Release support for collection of layer 7 data for DNS request fields by extending support for the collection of layer 7 data for DNS response fields as well, along with the export of DNS response-based L7 metadata to other Trellix products. • **Impact: Minor** • **Rationale: This was an update to a non-evaluated out-of-scope feature related to export of metadata to other Trellix products, that does not affect the evaluated TSF.** **SmartVision attacks:** The 11.1 Update 7 release includes SmartVision attacks, a new set of native IPS attack definitions containing attacks which generate base events that allow for more comprehensive and effective detection and correlation of network activities and potential threats, including the lateral movement of malware, when the integration between the Trellix IPS and Trellix NI (Network Investigator) devices is enabled. • **Impact: Minor** • **Rationale: This was an update to a non-evaluated out-of-scope feature related to integration with another Trellix device, that does not affect the evaluated TSF.** **GUI terminology updates:** The 11.1 Update 7 release includes minor updates to the GUI navigation for the 'L7 Data Collection' path. • **Impact: Minor** • **Rationale: This was a GUI terminology update to a non-evaluated out-of-scope feature, that does not affect the evaluated TSF.** **Sensor OpenSSL fix:**

	The 11.1 Update 7 release had the OpenSSL version on the Sensor devices upgraded from 1.0.2zj in the Update 6 release to 1.0.2zk, to cover a fix for CVE-2024-5535. • **Impact: Minor** • **Rationale: With OpenSSL 1.0.2 being out of support since January 2020, version 1.0.2zk was a premium support version released to only fix CVE-2024-5535 as mentioned on https://openssl-library.org/news/vulnerabilities/, with no other changes. Hence, it does not affect the evaluated TSF, as also confirmed during the vendor's pre-release QA and feature testing explained in Section** Error! Reference source not found. **of this document..**

Software Changes 11.1 Update 6:

Type of Change	Impact Analysis
New Features	None
Enhancements	**Public GTI communication interface upgrade:** Starting with the 11.1 Update 6 release, Trellix IPS uses ECHDE ciphers to connect to Public GTI (Global Threat Intelligence), which is Trellix's comprehensive, real-time, cloud-based reputation service, for IP and URL Reputation. This also included a CLI command update with GTI counters. • **Impact: Minor** • **Rationale: This was a minor enhancement to a non-evaluated out-of-scope feature related to the communication interface with another Trellix service, that does not affect the evaluated TSF.** **Support for import of multiple licenses in the Manager:** The Manager requires Sensor-specific license files to be imported in order to facilitate proper Sensor-Manager communicaton. Starting with the 11.1 Update 6 release, the Manager facilitates the import of multiple licenses (SKU files in the .zip format) through the System tab of the Licenses page in the Manager GUI. • **Impact: Minor** • **Rationale: This was a minor enhancement to an existing feature which has no relevant impact on the evaluated TSF.** **Syslog server configuration enhancement:** Starting with the 11.1 Update 6 release, an administrator can configure the syslog server timeout value in minutes using 'notifications.syslog.tcptimeout' in the 'advancedconfig.properties' file within the <Manager_Install_Dir>\App\Config folder, after which the Manager reconnects to the syslog server at the given intervals. If the time since the last connection re-establishment to the syslog server exceeds the configured timeout, the Manager will re-establish the connection before sending the syslog message. However, if 'notifications.syslog.tcptimeout' is not configured, the Manager will not reconnect once the trust has been established. After configuring 'notifications.syslog.tcptimeout', the Manager service must be restarted for the changes to take effect. • **Impact: Minor** • **Rationale: This was a minor enhancement to the existing implementation in order to keep refreshing the connection with the syslog server at regular intervals. Irrespective of the new timeout configuration, the TOE still re-attempts the connection in cases of loss of reachability. Hence, it does not affect the evaluated TSF.**

	Syslog message enhancement: Starting with the 11.1 Update 6 release, the IPS Manager can now send 16384 bytes in a single syslog message. This value was previously capped at a maximum of 8192 bytes wherein larger messages would be split into two or more syslog messages. • **Impact: Minor** • **Rationale: This was a minor enhancement to an existing feature which has no relevant impact on the evaluated TSF.** **Support for DNS protocol for layer 7 data collection:** Starting with the 11.1 Update 6 release, Trellix IPS supports collecting layer 7 data for DNS request fields and the export of the DNS request based L7 metadata to other Trellix products, such as Trellix Network Investigator (NI). • **Impact: Minor** • **Rationale: This was a minor enhancement to a non-evaluated out-of-scope feature related to export of metadata to other Trellix products, that does not affect the evaluated TSF.** **Capture Packets section enhancement:** Attack Definitions in Trellix IPS have a 'Capture Packets' section to support capturing of packets in post and pre-attack scenarios. Starting with the 11.1 Update 6 release, the fields in the Capture Packets section (for both Pre-Attack and Post-Attack) are set to disabled by default for all attacks of Informational and low severity levels, and not available for configuration for some specific attack IDs. This is done to prevent certain scenarios of excessive packet log generation. • **Impact: Minor** • **Rationale: This was a minor enhancement to an existing feature which has no relevant impact since it was not used or required in the evaluation of the IPS TSF.** **Update Server Request Enhancement:** Starting with the 11.1 Update 6 release, the Manager makes asynchronous requests to Trellix IPS Update Server, and in case of connectivity errors, it logs the error messages in the updateserver.log file for troubleshooting purposes. This is done to enhance the overall performance and stability of the Manager UI. • **Impact: Minor** • **Rationale: This was a minor enhancement to a non-evaluated out-of-scope feature related to automatic software updates, which was not claimed, and hence does not affect the evaluated TSF.** **Additional log files:** Starting with the 11.1 Update 6 release, several log files have been added for troubleshooting purposes, such as c3p0.log, c3p0monitor.log, alertRate.log, and packetlogRate.log. • **Impact: Minor** • **Rationale: This was a minor enhancement involving the addition multiple of log files, none of which are relevant to the in-scope TSF. Hence, it does not affect the same.** **Alert Pruning and Database Tuning enhancement:** Starting with the 11.1 Update 6 release, when data tuning gets triggered while the alert pruning operation is in progress, data tuning waits for permission and resumes after alert pruning is complete. Similarly, when alert pruning gets triggered while the data tuning operation is in progress, alert pruning waits for

	permission and resumes after data tuning is complete. This enhancement prevents overlapping and failure scenarios of data tuning and alert pruning. • **Impact: Minor** • **Rationale: This was an enhancement to non-evaluated out-of-scope features, that has no relevant impact on the evaluated TSF.** **CA-signed certificate file size enhancement:** Starting with the 11.1 Update 6 release, the file size of the CA certificate used for Sensor-Manager communication has been increased to support a maximum of 4096 bytes. This was capped at 2048 bytes earlier. • **Impact: Minor** • **Rationale: This was a minor enhancement to an existing in-scope feature which has no relevant impact on the TSF.** **GUI terminology updates:** The 11.1 Update 6 release includes minor updates to the GUI navigation for the 'Event Reporting' path under the 'Analysis' section. • **Impact: Minor** • **Rationale: This was a GUI terminology update to a non-evaluated out-of-scope feature, that does not affect the evaluated TSF.** **MariaDB Upgrade:** The Manager server operates with an RDBMS for storing persistent configuration information and event data, and uses MariaDB for the same. Starting with the 11.1 Update 6 release, the IPS Manager uses MariaDB version 10.11.6 instead of the previous 10.6.16 version, to include additional security against new vulnerabilities and bug fixes. • **Impact: Minor** • **Rationale: This version upgrade was for consuming the security fixes included in the quarterly library release. It has no relevant impact on the evaluated TSF, as also confirmed during the vendor's pre-release QA and feature testing explained in Section** Error! Reference source not found. **of this document.** **Apache Tomcat server upgrade:** The IPS Manager uses Apache Tomcat for its GUI web server implementation. Starting with the 11.1 Update 6 release, the Tomcat server used in the Manager is upgraded to version 9.0.88 from the previous 9.0.85 version. This update provides a collection of security fixes. • **Impact: Minor** • **Rationale: This version upgrade was for consuming the security fixes. It has no relevant impact on the dependent in-scope GUI functionality, as also confirmed during the vendor's pre-release QA and feature testing explained in Section** Error! Reference source not found. **of this document.** **Sensor OpenSSL fix:** The 11.1 Update 6 release had the OpenSSL version on the Sensor devices upgraded from the previous 1.0.2zh version to 1.0.2zj, to cover fixes included in this version, as well as the intermediate 1.0.2zi version, for CVE-2023-3446, CVE-2023-3817, CVE-2023-5678 and CVE-2024-0727. • **Impact: Minor**

	• **Rationale: With OpenSSL 1.0.2 being out of support since January 2020, version 1.0.2zj was a premium support version released to only fix the above-mentioned CVEs as mentioned on https://openssl-library.org/news/vulnerabilities/, with no other changes. Hence, it does not affect the evaluated TSF, as also confirmed during the vendor's pre-release QA and feature testing explained in Section** Error! Reference source not found. **of this document.** **Manager GUI HTTPS redirect:** Starting with the 11.1 Update 6 release, the Manager GUI no longer supports HTTP-based connections and can only be accessed via HTTPS with the user required to manually enter 'https://' before the hostname/host IP. Previously, any attempts to access the GUI via HTTP would be automatically redirected to HTTPS. Now, there will be no redirects and HTTP attempts simply won't load. • **Impact: Minor** • **Rationale: This was a minor enhancement to an existing in-scope feature which has no relevant impact on the evaluated TSF.** **Sensor OpenSSH patches:** Starting with the 11.1 Update 6 release, OpenSSH 7.8p1 on the Sensor incorporated patch fixes to fix CVE-2018-20685, CVE-2019-6109, CVE-2019-6110 and CVE-2019-6111. The version remains unchanged. • **Impact: Minor** • **Rationale: These patches were to consume the included security fixes for the above-mentioned CVEs, with no other changes. It has no relevant impact on the evaluated TSF, as also confirmed during the vendor's pre-release QA and feature testing explained in Section** Error! Reference source not found. **of this document.**

As per the previous evaluation documented in "Trellix Intrusion Prevention System Sensor and Manager Appliances version 11.1 Security Target, Version 1.9, May 14, 2024", together with this assurance continuity activity, the final set of claimed supported evaluated devices is:

Model	CPUs	Memory (Size and Qty)	Storage	Micro-architecture
Trellix Intrusion Prevention System Sensor Appliances				
IPS-NS9600	2 x XEON GOLD 5520+	12 x 32 GB	2 x 400GB SSD	Emerald Rapids
IPS-NS9500	2 x XEON GOLD 6230	12 x 16GB	2 x 240GB SSD	Cascade Lake
IPS-NS7600	1 x XEON SILVER 4416+	6 x 32GB	1 x 400GB SSD	Sapphire Rapids
IPS-NS7500	1 x XEON GOLD 5218N	6 x 16GB	1 x 240GB SSD	Cascade Lake
IPS-NS3600	1 x XEON D-1734NT	2 x 32GB	1 x 400GB SSD	Ice Lake
IPS-NS3200	1 x ATOM C2538	2 x 4GB	1 x 30GB SSD	Rangeley
Trellix Intrusion Prevention System Manager Appliance				
NSM-MAPL-NG	1 x XEON SILVER 4210	4 x 16GB	2 x 2TB HDD	Cascade Lake
NSM-MAPL -NG	1 x XEON SILVER 4114	4 x 16GB	2 x 2TB HDD	Skylake

Developer Testing

Regression/Release Testing
Trellix performs full functional testing, stress testing and regression testing for any newly released software version, with it being tested across all the hardware platforms to ensure TOE functionality is maintained and that newly introduced features or enhancements do not affect the security functionality previously tested and verified.

The functional testing verifies that the newly added features and enhancements behave as expected. The stress testing ensures that the product can handle the claimed traffic with full fidelity. The regression testing ensures that existing functionality is not broken due to any new feature implementation or bug resolution.

Certified Software Image Testing
In addition to the above, Trellix performs the below-mentioned security-relevant tests to ensure that the evaluated functionalities are working as expected.

- TLS:
  - Validation for supported and unsupported TLS versions using the OpenSSL utility.
  - Validation for supported and unsupported curves using the OpenSSL utility.
  - Validation for supported and unsupported cipheruites using the OpenSSL utility.
  - Validation for various combinations of signature algorithms using the OpenSSL utility.
- SSHC/SSHS:
  - Validation for supported and unsupported HostKeyAlgorithms using the OpenSSH utility.
  - Validation for supported and unsupported KexAlgorithms using the OpenSSH utility.
  - Validation for supported and unsupported Ciphers using the OpenSSH utility.
  - Validation for supported and unsupported HMAC hashing algorithms using the OpenSSH utility.
- FCS_TLSS_EXT.1 : Sample regression testing.
- FCS_TLSC_EXT.1: Sample regression testing.
- FIA_X509_EXT_1.1/Rev and FIA_X509_EXT_1.1/ITT: Sample regression testing.
- IPS_ABD_EXT.1 : Sample regression testing.
- IPS_IPB_EXT.1 : Sample regression testing.
- IPS_NTA_EXT.1 : Sample regression testing.
- IPS_SBD_EXT.1 : Sample regression testing.
- FPT and FTP classes: Sample regression testing.

Internal Feature Regression Coverage (Automated):

- SSL_INBOUND SUITE
- SSL_INBOUND_PROXY SUITE
- SSL SUITE

- EVASIONS SUITE
- PROTECTION_OPTIONS SUITE
- MALWARE SUITE
- HTTP2 SUITE
- ATDT_CLI_MEM SUITE
- CUSTOM_ATTACK_ADV_SCAN SUITE
- TRAFFIC_MANAGEMENT_RECON SUITE
- MISCELLANEOUS SUITE
- APPID SUITE
- LOGGING SUITE
- INTEGRATION SUITE

Assurance Activity Requirements
No changes were made to the Security Functional Requirements.

Below is a summary of the Security Assurance Requirement changes:

Assurance Family	Description of Evidence Changes
ASE	Only the TOE version number has changed in the ST, along with the inclusion of the new Sensor platform.
ALC_CMC.2 ALC_CMS.2 AGD_OPE.1 AGD_PRE.1	Only the incorporation of the new features and enhancements, updates to mentions of Sensor and Manager versions and inclusion of mention of the new IPS-NS9600 Sensor platform has changed in the AGD
AVA_VAN.1	Only some of the TOE libraries have changed, and an entirely fresh search for public vulnerabilities was done using the revised keywords.
ATE	None

No other SARs are affected.

NIST CAVP Certificates:
The newly added IPS-NS9600 Sensor Platform with Intel Xeon Gold 5520+, Emerald Rapids operating environment has been added to the CAVP certs claimed in the original evaluation (A3350, A3353). Therefore, the original CAVPs cover all TOE operating environments claimed in this Assurance Maintenance action and no reverification of the certificates is necessary.

Vulnerability Analysis:
This Vulnerability Analysis documents the review performed by Acumen for the TOE as specified in the Collaborative Protection Profile for Network Devices, Version 2.2e and PP-Module for Intrusion Protection Systems (IPS), Version 1.0.

In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined are as follows:

- https://nvd.nist.gov/view/vuln.search

- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities
- https://thrive.trellix.com/

The evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor's name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Trellix Intrusion Prevention System 11.1
- Trellix Intrusion Prevention System 11.1 Update 7.
- Trellix IPS Manager.
- Trellix IPS Sensor.
- Trellix NS3200.
- Trellix NS3600
- Trellix NS7500.
- Trellix NS7600.
- Trellix NS9500.
- Trellix NS9600
- Intel XEON GOLD 6230.
- Intel XEON GOLD 5218N.
- Intel ATOM C2538.
- Intel XEON SILVER 4210.
- Intel XEON SILVER 4114.
- Intel XEON SILVER 4416+
- Intel XEON D-1734NT
- Intel XEON GOLD 5520+
- MLOS 3.9.
- McAfee Linux Operating System 3.9.
- Apache Tomcat 9.0.88
- MariaDB 10.11.6
- BouncyCastle 2.2.0

- OpenSSL 1.0.2zh
- OpenSSL 1.0.2zk
- OpenSSL-fips 2.0.5
- OpenSSH 7.4P1-33
- OpenSSH 7.8p1
- Rsyslogd 8.24.0-57

The vulnerability search was performed on 29th January 2025. No open vulnerabilities applicable to the TOE were identified.

Conclusion:
The evaluation evidence consists of the Security Target and CC-specific Guidance Documentation. Both the Security Target and Guidance Documentation were revised to include the additional TOE sensor model and software version. The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims.

There are no changes to TSF Interfaces, no SFR changes, no changes to assumptions threats or objectives and no CAVP changes. Regression testing was done, and an equivalency argument was provided justifying how the new TOE model was considered equivalent to the TOE models tested during the original evaluation. The reasoning is considered adequate based on the scale and types of changes made. The vulnerability search also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. The impact of all TOE changes on the assurance baseline is assessed to have an impact of minor severity and is within the parameters of the Assurance Continuity Framework.

In review of the changes between TOE versions, no change has been made that impacts the evaluated configuration of the TOE. The product properly maintained conformance to the protection profile while performing regular updates to ensure bug fixes were addressed. No changes made to the product across revisions impacts the functionality claimed within the original Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.