ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Trend Micro TippingPoint Threat Protection System (TPS) v5.3

Maintenance Update of Trend Micro TippingPoint Threat Protection System (TPS) v5.3

Maintenance Report Number: CCEVS-VR-VID10949-2020

Date of Activity: 13 April 2020

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Trend Micro TippingPoint Threat Protection System (TPS) v5.3 Impact Analysis Report, Version 1.0, 7 April 2020
- Trend Micro TippingPoint Threat Protection System (TPS) v5.2 Impact Analysis Report, Version 1.0, 15 October 2019
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.0E + Errata 20180314, March
- ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Trend Micro TippingPoint Threat Protection System (TPS) v5.2, 6 November 2019

Assurance Continuity Maintenance Report:

Leidos, submitted an Impact Analysis Report (IAR), for the Trend Micro TippingPoint Threat Protection System, to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 20 March 2020. 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 configuration guide, the Command Line Interface Reference, and the Impact Analysis Report (IAR). The ST, guide document, and the IAR were all updated. The Command Line document was new.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Trend Micro TippingPoint Threat Protection System (TPS) v5.2 Security Target	The ST was changed to update the software version to 5.3. The version of the Linux distribution included in TPS was updated to Linux-4.14.76-yocto. A typographic error in Section 6.2, which referred to the version of OpenSSL included in TPS as '1.0.2i-fips', was corrected to '1.0.2l-fips'. Document references were modified to reference updated administrative guidance and the new version/date of the ST.
Guidance: • Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, November 2019 • Trend Micro Common Criteria Evaluated Configuration Guide (CCECG) for TPS v5.2	New features or changes arising from addressed issues were described in the updated guidance where necessary, e.g., the CLI reference includes appropriate notes/warnings that a valid hostname consists only of alpha-numeric characters and hyphens and cannot exceed 63 characters. Aside from mentioning the updated TOE software and new TOE hardware models, there are no security-relevant changes to the CCECG.

Changes to TOE:

For this Assurance Continuity, the following TOE updates were released:

New Features in Version 5.3	Impact
The Linux kernel distribution included in TPS v5.3.0 has been updated to Linux-4.14.76-yocto-standard.	**Minor change:** Updates that have been made to the Linux kernel between version 4.4 and 4.14 involved improvements to low level kernel performance or new features that are not used by TPS and not relevant to the evaluated configuration (such as support for new non-Intel processor architectures or new device drivers). This change requires only minor updates to relevant documentation, to identify the updated Linux kernel version, and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing. In addition, the updated vulnerability search did not identify any issues related to the Linux kernel that were applicable to the TOE.

This release introduces support for multiple certificates and keys for a single TLS server. Support for the Server Name Indication (SNI) protocol extension enables the server to host multiple TLS certificates (up to 1,000 per device) for multiple sites under a single IP.	**Minor change:** The TOE in its evaluated configuration does not support TLS communication. All communication, either for remote administration (FTP_TRP.1) or for exporting audit records to an external audit server, is over SSH. As such, this change is outside the scope of the evaluated TOE and therefore minor.
This release introduces new CLI commands for managing core files: • To remove core files: delete corefiles • To include or exclude core files in a tech support report: include corefiles | exclude corefiles	**Minor change:** There are no requirements for, nor restrictions on, the management of core files specified in the claimed Protection Profile. As such, this change is outside the scope of the evaluated TOE and therefore minor.
This release increases the number of cipher suites supported for SSL inspection from 11 to 14. The following are the three additional cipher supported in v5.3: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256.	**Minor change:** SSL inspection is not in the scope of the TOE as it does not relate to the functionality defined in the claimed Protection Profile. As such, this change is outside the scope of the evaluated TOE and therefore minor.
This release improves SNMP by including support for or enhancements to the following MIBs: TPT-POLICY TPT-HOST TPT-LICENSE TPT-MULTIDV	**Minor change:** The TOE in its evaluated configuration does not support SNMP communication. All communication, either for remote administration (FTP_TRP.1) or for exporting audit records to an external audit server, is over SSH. As such, this change is outside the scope of the evaluated TOE and therefore minor.
Issues Addressed in Version 5.3	**Impact**
The LSM interface for configuring SSL has been removed. Use the SMS Client interface to configure SSL. SSL inspection active session information has been removed from both the LSM and SMS.	**Minor change:** The LSM (Local Security Management) component is explicitly excluded from use in the evaluated configuration (see Section 2.2.1.3 of the ST). Likewise, the SMS (Security Management System) is excluded from the evaluated configuration (see Section 2.1 of the ST), and SSL inspection is not an evaluated function. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.

System logs now indicate when a device is forced into a cold reboot.	**Minor change:** The TOE already generates audit records for start-up and shut-down of the audit function. Auditing of cold reboots of the TOE is not covered by, nor required by, the audit generation requirement (FAU_GEN.1) in the PP. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
Data no longer stalls on long-lasting persistent connections with infrequent traffic going through SSL inspection.	**Minor change:** SSL inspection is not an evaluated function. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
Enterprise Vulnerability Remediation (eVR) scans now support non-ASCII characters in filenames.	**Minor change:** eVR scans are not evaluated functionality. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
Adding or deleting inspection bypass rules no longer causes the remaining rules to be reordered differently than the way they were listed in the original configuration.	**Minor change:** The use of inspection bypass rules is not evaluated functionality. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
Placing an inspection bypass rule with an ingress-mirror action first in the rule order no longer changes the behavior of subsequent rules.	**Minor change:** The use of inspection bypass rules is not evaluated functionality. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
The documentation has been updated to clarify that users with Administrative privileges can view and clear the audit logs for TPS devices.	**Minor change:** This was only a change to product documentation. The Superuser and Admin roles have always had the ability to view the audit logs (functionality not covered by the PP) and to clear audit logs (i.e., delete the entire audit trail, not individual audit records), which is covered by testing in the original evaluation. The resolution of this issue does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
RX and TX power readings have been added to the debug np port diag command. The readings are updated every few seconds for supported transceivers.	**Minor change:** Use of the debug command is not covered in the scope of the original evaluation. The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be

	necessary beyond the vendor's standard regression testing.
The TPS and SMS interfaces no longer permit hostnames to include periods (.). Hostnames can consist only of alpha-numeric characters and hyphens and cannot exceed 63 characters or have a hyphen at the beginning or end.	**Minor change:** The resolution of this issue does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.
A condition that caused the TPS to slowly consume internal memory has been resolved.	**Minor change:** This is a performance-related issue whose resolution does not require any changes to relevant documentation and does not affect security functionality such that specific testing would be necessary beyond the vendor's standard regression testing.

No functionality, as defined in the SFRs, was impacted, and none of the software updates affected the security functionality or the SFRs identified in the Security Target.

All updates are, therefore, considered to be Minor Changes.

Regression Testing:

Trend Micro follows a standard process for bug tracking and flaw remediation. A key element of this process is product regression testing.

For each bug that is identified or reported and for which a fix is to be developed, Trend Micro identified a release target. Once a release target was selected, development and quality assurance (QA) resources was scheduled to resolve the bug and verify the fix. Members of the QA group verified the fix by configuring the affected feature and duplicating the reported issue. Following this specific feature-level verification, QA ran an automated test suite to verify that no other features have been affected by the fix. Lastly, a longevity test was run for several days to further identify problems.

NIST CAVP Certificates:

No changes to any NIST Certs were required. The change to Linux-4.14.76-yocto-standard from Linux version 4.4 involved no changes to the underlying openssl libraries, did not invalidate existing NIST Certs, and was only a "minor" revision tracking number change.

Vulnerability Analysis:

A public search for vulnerabilities that might affect the TOE was performed on March 17, 2020, and the results were compared to the vulnerability analysis performed for TPS v5.2, dated October 4, 2019 and described in the previous section. In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the updated version of the TOE.

Search Terms:

- “TippingPoint”
- “threat protection”
- “TCP”
- “SSH”
- “openssh”
- “openssl”
- “linux (kernel)”

No residual vulnerabilities for found for any of the search terms.

Conclusion:

Since none of the updates to the TOE changed the functionality and the regression testing produced the correct results, the overall update to the TOE can be considered Minor. In addition, an updated Vulnerability search was done that found that no un-remediated vulnerabilities existed, and the existing NIST Certs did not require any updates or changes.

Therefore, CCEVS agrees that the original assurance is maintained for the product.