ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Trellix Endpoint Security (HX) Agent v36.30.17

Maintenance Update of Trellix Endpoint Security (HX) Agent v35.31.31

Maintenance Report Number: CCEVS-VR-VID11415-2026

Date of Activity: 03 June 2026

References:

- Common Criteria "Assurance Continuity: CCRA Requirements", version 3.1, February 2024.
- National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme Publication #6 Assurance Continuity: Guidance for Maintenance and Re-evaluation, v3.0, 12 September 2016
- Trellix Endpoint Security (HX) Agent Impact Analysis Report, Version 0.1, 16 December 2025.
- Trellix Endpoint Security (HX) Agent v36.30.17 Security Target, Version 2.4, November 10, 2025
- Trellix Endpoint Security (HX) Agent v36.30.17 Common Criteria Guidance Supplement, Version 1.5, November 17, 2025
- Equivalency Analysis for Trellix Endpoint Security (HX) Agent v36.30.17, Version 0.1, November 25, 2025
- xAgent Deployment Guide, Version 36.30.17, December 10, 2025
- Vulnerability Assessment for Trellix Endpoint Security (HX) Agent v36.30.17, Version 1.2, June 01, 2026
- Protection Profile for Application Software, Version: 1.4, October 7, 2021
- Functional Package for Transport Layer Security, Version 1.1, March 1, 2019

Documentation Updated:

- **Security Target:** Trellix Endpoint Security (HX) Agent v36.30.17 Security Target, version 2.4, November 10, 2025
    - Changes in the maintained ST are:
        - Updated identification of ST
        - Section 1.1 - Updated TOE software version
        - Section 1.4.1 – Updated TOE platform to remove Windows 10, Windows Server 2008 & 2012, and ESXi v7.0; Add Windows 11 (21H2) and ESXi v8.0
        - Section 1.4.3 – Updated AGD documentation to latest versions.

    - Section 6.2.6.4 – Third-party libraries updated to include newer version of OpenSSL (3.3.1) and the removal of unused Visual Studio runtime libraries.
- **Common Criteria Compliance Guide**: Trellix Endpoint Security (HX) Agent v36.30.17 Common Criteria Guidance Supplement, version 1.5, November 17, 2025
    - Changes in the maintained Guidance are:
        - Updated TOE version from v35.31.31 to v36.30.17, both in textual and image mentions of the version (screenshots).
        - Replaced the End-Of-Life ESXi 7.0 Hypervisor with the supported hypervisor ESXi 8.0.
        - Removed the listing of End-Of-Life Windows platforms as supported platforms.
        - Added a new supported host platform: Windows 11 25H2 64-bit running on ESXi Hypervisor v8.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- **Administration Guide**: xAgent Deployment Guide, Version 36.30.17, December 10, 2025
    - Updated TOE version from v35.31.31 to v36.30.17.

Assurance Continuity Maintenance Report:

Acumen Security submitted an Impact Analysis Report (IAR) on behalf of Musarubra US LLC ("Trellix") and the Trellix Endpoint Security (HX) Agent v36.30.17 to CCEVS for approval in December 2025. The IAR is intended to satisfy requirements outlined in Common Criteria document “Assurance Continuity: CCRA Requirements”, version 3.1, February 2024. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

Changes to TOE:

The changes described in this document constitute all changes made to the Trellix Endpoint Security (HX) Agent v36.30.17 since the previous Common Criteria evaluation (CCEVS-VR-VID11415-2024). The previous evaluation tested the TOE on the following specific platforms:

- Windows 10 Version 21H2 32-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 10 Version 1803 32-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 10 Version 1903 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 10 Version 1909 LTSC 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620V4 processor (Broadwell).
- Windows 10 Version 2004 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 10 Version 21H2 64-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 10 Version 1803 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 10 Version 1903 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).

- Windows 10 Version 1909 LTSC 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620V4 processor (Broadwell).
- Windows 10 Version 2004 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).
- Windows 11 Version 21H2 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).
- Windows Server 2016 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2019 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2012 R2 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2008 R2 (SP1) running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4processor (Broadwell).
- Windows Server 2022 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).

The Trellix Endpoint Security (HX) Agent v36.30.17 is now supported on the following platforms.

- Windows 11 Version 21H2 64-bit running on ESXi Hypervisor v8.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 11 Version 25H2 64-bit running on ESXi Hypervisor v8.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2016 running on ESXi Hypervisor v8.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2019 running on ESXi Hypervisor v8.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows Server 2022 running on ESXi Hypervisor v8.0 on Intel Xeon E5-4620 V4 processor (Broadwell).

Platform equivalency between ESXi v7.0 and ESXi v8.0 is established by the fact that there is no change to the claimed processor architectures (Intel Xeon E5-4620 V4) and no utilization by the TOE of the underlying hypervisor platform. Operating System equivalency between the newly claimed Windows 11 version 25H2 and previously evaluated and listed versions 24H2 and 23H2 is established by virtue of all versions of Windows 11 sharing the same kernel (version 10.0) and no changes are being claimed in the processor architectures. The validators judge these changes to be minor.

The Trellix Endpoint Security (HX) Agent v36.30.17 software was updated from version 35.31.31 to version 36.30.17. The updates are summarized below.

1. Support for new platforms including Ubuntu 24.04, macOS 15.2 and 15.3.1, and Windows Server Core 2025. Linux and Mac platforms are out of scope for the evaluated configuration. The change is considered to be minor.
2. New audit features to enable multiple file acquisitions and changes to audit agent settings. These changes affect non-TSF areas of functionality and are considered minor.

3. OpenSSL upgrade to version 3.3.1. This update consolidated several applicable CVE's and maintained the current version for the FIPS provider (3.0.8). The change is considered to be minor.
4. FPT_LIB_EXT.1 updated to map DLL files to corresponding libraries and remove Visual Studio DLL files because they are not used implement any TSF functionality. The change is considered to be minor.
5. Package dependencies within the Linux Real-Time event sensor (rte-sensor) were updated to patch applicable CVEs. Linux platform is not claimed. The change is considered to be no impact.
6. Linux Agent rte-sensor binary Golang updated to version 1.20.4. Linux platform is not claimed. The change is considered to be no impact.

Regression Testing:

Although only minor changes were made to the functionality of the TOE, regression testing by the evaluation security team on the new hardware platforms demonstrated that the TOE functionality was equivalent to the original evaluated configuration and unchanged from previous evaluations. New test results were generated and were reviewed by Vendor. Testing evidence was attested to by the evaluation security team in the IAR and was reviewed by the validators.

Vulnerability Assessment:

The evaluation team conducted new vulnerability searches in support of this ACMR. The most recent search was conducted on June 01, 2026, and used the following sources:

- https://nvd.nist.gov/vuln/search
- https://www.cve.org/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://thrive.trellix.com/s/customknowledge

Search terms and keywords were relevant to the TOE and TSF functionality and are documented in the Vulnerability Assessment for Trellix Endpoint Security (HX) Agent v36.30.17 document. The terms are not reproduced here.

No open vulnerabilities applicable to the TOE were identified.

Conclusion:

The specific changes identified in this ACMR to the product are considered minor and do not affect the security claims in the Trellix Endpoint Security (HX) Agent v36.30.17 Security Target. While the SFR FPT_LIB_EXT.1 was modified, the change does not impact the TSF. There were no other changes to SFRs, Security Functions, Assumptions or Objectives. The security target and the Common Criteria Evaluation Guidance Document are updated to reflect the updates.

Test results were declared by the evaluation security team to be consistent with the previous test results. The evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. The search did not identify any new potential vulnerability.

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.