ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12

Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12

Maintenance Report Number: CCEVS-VR-VID11456-2025
Date of Activity: June 18, 2025
References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, 12 September 2016
- *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Impact Analysis Report*, Version 1.1, June 17, 2025
- *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.3, May 6, 2025
- *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 1.0, May 6, 2025
- *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Detailed Test Report Evidence WLC-CL*, Version 1.0, May 23, 2025
- *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Vulnerability Assessment*, Version 1.1, June 17, 2025
- *collaborative Protection Profile for Network Devices*, Version 2.2e, March 23, 2020 (NDcPP22e)
- *PP-Module for Wireless Local Area Network (WLAN) Access System*, Version 1.0, March 31, 2022

Assurance Continuity Maintenance Report:

Lightship Security submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package to the CCEVS for approval in May 2025 on behalf of Cisco Systems, Inc. The IAR is intended to satisfy the 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 (ST), the Administrator's Guide, the Detailed Test Report Evidence, the Vulnerability Assessment and the Impact Analysis Report (IAR).

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.2, April 6, 2025	**Maintained Security Target:** See references above. • Updated reference to the AGD to *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 1.0, May 6, 2025. • TOE virtual appliance (C9800-CL-K9) hypervisor changed from ESXi6.7 to ESXi 8.0. • Document version: Security Target updated to *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Security Target*, Version 1.3, May 6, 2025.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 0.9, April 6, 2025	**Maintained Guidance Documentation:** See references above. • Instructions to configure the virtual appliance changed from referring to ESXi 6.7 to ESXi 8.0. • Document version: AGD updated to *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 CC Configuration Guide*, Version 1.0, May 6, 2025.
Lifecycle: None	No changes required.
Testing: None	**Maintained Test Evidence Documentation:** See references above. A subset of testing was performed on the WLC-CL virtual appliance running IOS 17.12.04 on a Cisco UCSC-C220-M5SX V03 server running ESXi 8.0 update 3e. This subset of tests was selected to validate any behavioral changes that might be provided by virtualized components. The testing did not

	produce any different results from what was expected.
Vulnerability Assessment: *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Vulnerability Assessment*, Version 1.1, April 6, 2025	**Maintained Vulnerability Assessment Documentation:** See Evidence above. • The public search was updated on June 17, 2025. No public vulnerabilities exist in the product. See analysis results below. • Document version: VA updated to *Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 Vulnerability Assessment*, Version 1.1, June 17, 2025.

Changes to TOE:
No changes were made to the TOE.

Major Changes

None.

Minor Changes

None.

Changes to the TOE Operational Environment:

Major Changes

None

Minor Changes

Changed Hypervisor Host Version. The hypervisor that the TOE virtual appliance ran on was changed from ESXi 6.x to ESXi 8.0. ESXi 6.7 is past End-Of-Life with the vendor no longer providing ongoing security patching. NIAP allowed the previous evaluation to complete but instructed the lab and vendor to come in for assurance maintenance within 120 days with a supported version of ESXi.

The virtual hardware version sets the compatibility of the virtual machine on the underlying hypervisor with respect to any included virtual hardware, settings, and resource limits. This includes:

- Use of UEFI for secure boot
- Virtual BIOS capabilities and settings
- vCPU behaviour
- The type of virtual video card used for implementing the virtual console
- Virtual drivers to access the virtual hard disk and virtual networking devices
- Access to advanced configuration parameters, as needed

Testing:
A test subset was selected to validate any behavioral changes that might be provided by virtualized components:

1) FAU_STG_EXT.1 Test 2 – selected because it directly stores a volume of non-volatile storage mediated by the PVSCSI paravirtualized device.
2) FIA_UAU.7 Test 1 – selected because it requires the local console and associated virtual graphics driver to be exercised.
3) FPT_STM_EXT.1 Test 1 - selected because it makes use of a clock mechanism which would possibly rely on a virtual machine reference clock provided by the hypervisor and we want to ensure that it is not interfering.
4) FPT_TST_EXT.1 Test "Self-Test Verification" – selected because UEFI booting on the virtual appliance enables the boot-up integrity firmware test. Support for UEFI boot is a feature provided by the underlying hypervisor.
5) FIA_8021X_EXT.1 Test 1 – selected to ensure that all virtual machine network interfaces are working as expected.

The testing did not produce any different results from what was expected.

Equivalency:
The security functionality of the Cisco Catalyst 9800 Series Wireless Controllers and Access Points 17.12 remains the same as the original evaluation. The hardware platforms are unchanged from the previous maintained version.

NIST CAVP Certificates:
CAVP certificates A4595 (for Cisco FOM 7.3) and A3244 (for IOS Common Cryptographic Module) were updated to add Intel Xeon Platinum 8160M (Skylake) Linux 5 w/ ESXi 8.0 as an Operational Environment (OE). A certificate review was performed using the evidence in the updated Evaluation Technical Report and both certificates were found to be acceptable.

Vulnerability Analysis:
An updated vulnerability analysis was performed on June 17, 2025, using the original search terms and included ESXi 8.0. No applicable vulnerabilities were found.

Conclusion:
CCEVS reviewed the description of the changes and the analysis of the impact upon security and found the changes to be minor and did not affect the evaluated security functionality. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

The overall impact is minor. This is based on the rationale that updates to the TOE OE do not change any security policies of the TOE and are unrelated to SFR claims. The updates described above were made to support the new TOE OE.

Testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, a cert review was performed to ensure it covered the new OE. Therefore, CCEVS agrees that the original assurance is maintained for the product.