CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Gigamon GigaVUE v6.1 (CPP_ND_V2.2E)

Maintenance Report Number: CCEVS-VID11314-2023

Date of Activity: June 8, 2023

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3.0, September 12, 2016

NIAP Policy #12 “Acceptance Requirements of a product for NIAP Evaluation.” 29 August 2014.

Common Criteria document 2012-06-01 “Assurance Continuity: CCRA Requirements” Version 2.1, June 2012

Collaborative Protection Profile for Network Devices Version 2.2e 20200327 [NDcPP]

Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-001

Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-002

Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-003

Gigamon GigaVUE v6.0 Common Criteria Security Target, Version 1.0, February 3, 2023

Gigamon GigaVUE v6.0 Evaluation Technical Report (ETR) Version 1.0, February 3, 2023

Common Criteria Evaluation and Validation Scheme Validation Report Gigamon GigaVUE v6.0, Version 1.0, February 14, 2023

Affected Evidence:

Gigamon GigaVUE v6.0 Common Criteria Security Target, Version 1.0, February 3, 2023

Updated Developer Evidence:

- Security Target – The Security Target document below was updated to be applicable to the updated versions of the TOE for version 6.1:
    - Gigamon GigaVUE v6.1 Common Criteria Security Target v2.0 dated May 5th, 2023. Updates include:
        - Identification of the Changed TOE version
        - Security Target dates and versioning
- Guidance Document – The guidance document below was updated to be applicable to the updated versions of the TOE for versions 6.1:
    - Gigamon GigaVUE v6.1 Supplemental Administrative Guidance v2.0 dated May 5th, 2023.
        - Identification of the Changed TOE version
        - Update of document dates and versioning
        - Update of references to Changed TOE Security Target and other guidance documentation
        - Minor grammatical fixes

Description of ASE Changes:

The Security Target document below was updated to be applicable to the updated versions of the TOE for version 6.1:

- Gigamon GigaVUE v6.1 Common Criteria Security Target v2.0 dated May 5th, 2023. Updates include:
    - Identification of the Changed TOE version
    - Security Target dates and versioning
- The following sections in the ST were updated to reflect the changed TOE version:
    - 1.1 ST Reference,
    - 2.4 Physical Boundary, and the document cover page.
- The following sections of the ST were updated to reflect changed dates and document versioning:
    - 1.1 ST Reference,
    - 3.2 CC Part 2 Conformance Claims,
    - 3.3 CC Part 3 Conformance Claims, and the document cover page.

Changes to TOE:

Category	Number of Changes	Applicability to New
New Features	29	The new features added are part of the GigaVUE cloud suite and GigaVUE FM (Fabric management interface) which are separate products and outside the scope of the evaluation. These new features non-security relevant. The new features did not change how the TSF performed and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target.
Bug Fixes	37	36 of the bug fixes were considered non-security relevant and did not change how the TSF performed and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target. Bug fixes in areas related to TSF functions were not considered as part of the TSF of the updated configuration, because there are no SFRs that apply to the TSF or because the bug fix was not considered part of the TSF for the original evaluated configuration. One bug fix addressed recently discovered vulnerabilities resulted in focused regression testing.

Description of ALC Changes:

From version 1.0 to 2.0 of the Guidance Document

- Gigamon GigaVUE v6.0 Supplemental Administrative Guidance v2.0, February 3, 2023.
- Gigamon GigaVUE v6.1 Supplemental Administrative Guidance v2.0, May 5, 2023.

The following sections in the AGD were updated to reflect the changed TOE version

- 1 Introduction,
- 2 Intended Audience,
- 4 References,
- 6.3 Configure the TOE to use Secure Cryptography Mode, and the document cover page.

The following sections of the AGD were updated to reflect changed dates and document versioning

- The document cover page.

References to the Changed ST and other guidance documentation were made in the following sections:

- 4 References and references to page numbers throughout,
- 7 Secure Management of Gigamon GigaVUE.

Minor grammatical fixes were made to the following sections of the Guidance Document:

- 1 Introduction,
- 3 Terminology,
- 5.2 Supporting Environment Components,
- 6.1 Initial Out-of-the-Box Setup,
- 6.3 Configure the TOE to use Secure Cryptography Mode,
- 6.5 Disable/Enable Service,
- 7.8 Secure Updates, and
- 9 Communication Protocols and Services.

Assurance Continuity Maintenance Report:

Booz Allen Hamilton submitted an Impact Analysis Report (IAR) dated 06/08/2023 to incorporate new features and bug fixes into the product.

- The new features did not change how the TSF performed and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target.
- The bug fixes did not change how the TSF performed and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target. There were no negative impacts due to bud fixes and no documentation needed to be updated.

- There was no change to the operational environment for the evaluated configuration of the TOE. Therefore, the TOE environment for Gigamon GigaVUE 6.1 presents no impact to the overall evaluation.

Description of Regression Testing:

Gigamon's Quality Assurance team performed a full suite of tests to verify that the code changes were properly implemented and do not affect any of GigaVUE's other functionalities. Gigamon's regression testing on Gigamon GigaVUE v6.1 (Changed TOE) demonstrated that the behavior of the TSF remained consistent with the testing results obtained during the original evaluation. Regression test results confirm that the new features and bug fixes had no effect on any security-related functionality of the TOE.

Vulnerability Assessment:

Booz Allen Hamilton searched the Internet for potential vulnerabilities in the TOE using the six web sites listed below.

- NIST National Vulnerability Database (NVD, https://nvd.nist.gov/),
- MITRE Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org/cve/),
- United States Computer Emergency Readiness Team (US-CERT, http://www.kb.cert.org/vuls/html/search)
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Booz Allen Hamilton selected the 23 search key words based upon the vendor's name, the product(TOEs) name, general technology product terms, and libraries compiled with the TOE.

The search terms used were:

- Gigamon
- GigaVUE
- HC1
- HC-1
- HC2
- HC-2
- HC3
- HC-3
- TA25
- TA-25
- TA200
- TA-200
- GTAP
- CentOS (5.8)

- CentOS (7.6)
- OpenSSL (1.0.2zh)
- OpenSSH (8.8p1)
- Intel Atom C2758 (Rangely)
- Intel Atom C2538 (Rangely)
- Intel Xeon D1527
- QorIQ (P2041E)
- Intel Atom (C3338) (Denverton)
- Intel Atom (3538) (Denverton)

The IAR contains the output from the vulnerability searches since the original evaluation search dated February 3, 2023 and the rationale why the search results are not applicable to the TOE. This search was performed on June 6, 2023. There were no open or unpatched known vulnerabilities to the TOE or the libraries used by the TOE as a result of the public search.

Vendor Conclusion:

The 'Global Impact to Evidence' section (Chapter 8) of the details the global impacts that apply to the vendor evidence based on the Common Criteria documentation for assurance continuity.

All of the new features were considered non-security relevant because they represent changes to functionality that was not included as part of the TSF, products and features that were not in scope of the evaluation or were considered to be general performance/diagnostic/stability issues that were unrelated to security.

All but one of the bug fixes were considered non-security relevant because they represent changes to functionality that was not included as part of the TSF, products and features that were not in scope of the evaluation or were considered to be general performance/diagnostic/stability issues that were unrelated to security. One bug fix, that addressed recently discovered vulnerabilities, resulted in focused regression testing. Results of this focused regression testing validated that there were no negative impacts on the previously claimed functionality.

The CAVP certificates have not been impacted by the updates added to the Changed TOE.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updated Security Target and Supplemental Administrative Guidance for the Validated TOE received minor updates to address the Changed TOE to include product and document version updates. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.