CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1300, CSG1500, CSG2500, CSG3500, CSG5000, CSG5200, Dell PowerEdge R7515, Dell PowerEdge R7615, Dell PowerEdge XR5610, Dell VEP1445, Dell VEP1485, and Dell VEP4600 Versa Director 22.1, and Versa Analytics 22.1

Maintenance Report Number: CCEVS-VR-VID11431-2025

Date of Activity: March 17, 2025

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

Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1300, CSG1500, CSG2500, CSG3500, CSG5000, CSG5200, Dell PowerEdge R7515, Dell PowerEdge R7615, Dell PowerEdge XR5610, Dell VEP1445, Dell VEP1485, and Dell VEP4600 Versa Director 22.1, and Versa Analytics 22.1 Security Target Version 2.0 January 23, 2025

Impact Analysis Report for Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1300, CSG1500, CSG2500, CSG3500, CSG5000, CSG5200, Dell PowerEdge R7515, Dell PowerEdge R7615, Dell PowerEdge XR5610, Dell VEP1445, Dell VEP1485, and Dell VEP4600 Versa Director 22.1, and Versa Analytics 22.1 Revision 1.0 02/28/2025

collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)

PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)

PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)

PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3

PP-Configuration for Network Device, Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways v1.2

Affected Evidence:

Versa Networks Versa Secure SD-WAN Versa Operating System (VOS) 22.1 running on CSG1500, CSG2500, CSG3500, CSG5000, Dell PowerEdge R7515, and Dell VEP4600, Versa Director 22.1, and Versa Analytics 22.1 Security Target, version 1.9, 03/28/2024

Versa Operating System (VOS), Versa Director and Versa Analytics Version 22.1 Common Criteria Hardening Guide

Updated Developer Evidence:

This assurance maintenance request is to add seven new hardware models, and incorporate a number of software bug fix changes. The developer has provided sufficient supporting rationale describing the impact of each change. Both the Security Target and the Guidance Document were updated to identify the new hardware models.

Description of ASE Changes:

Gossamer Security Solutions (GSS) submitted an Impact Analysis Report (IAR #1) to CCEVS, on behalf of Versa Networks for approval to seven new hardware models, and incorporate a number of software bug fix changes. The new hardware platforms are the Versa CSG5200, Dell PowerEdge R7615, Dell VEP1445, Dell VEP1485, and Dell PowerEdge XR5610. These platforms are added to address manufacturer support lifecycle constraints with existing certified Dell hardware platforms, and to certify the brand-new Versa CSG5200 series which is an update to the CSG5000. In addition, the lower end CSG1300 is added. The new platforms do not provide any new features or changes in the TSF.

The new models required the addition of 4 new processors, AMD EPYC 9654P (Zen 4), Intel Atom C3758 (Goldmont), Intel Atom C3958 (Goldmont), and Intel Xeon Silver 4514Y (Emerald Rapids). These processors were added to 2 of the existing evaluated approved CAVPs, A5144 and A5147. The IAR provided the required evidence that the processors were sufficiently tested and that the CAVPs supported the processors and microarchitectures.

Changes to TOE:

The only changes to the TOE were the addition of seven new hardware models, and incorporation of a number of software bug fix changes. Most of the software changes had no impact on the evaluated configuration. Those software changes that did, had only minor impact. The changes that had minor impact were either performance enhancements, allowed the new hardware to be recognized, did not change security profile of trusted procedures, or addressed AVA vulnerabilities. The software changes are divided into three groups; VOS bug fixes, Director bug fixes, and Analytic bug fixes.

These software changes are summarized here:

- VOS bug fixes: 78 have no impact on the evaluated configuration and 11 have only minor impact. Of these, one is merely to allow the new hardware to be recognized, one fix merely introduces a short delay in the IPSec rekey processing to account for an edge case, one is a performance enhancement, two are changes that leave the trusted update procedures unchanged, two are for AVA_VAN vulnerabilities addressed by this release, and four have no impact to previously tested behavior.

- Director bug fixes: 82 have no impact and 8 have only minor impact. Of these, one is merely to allow the new hardware to be recognized, one is to allow passwords to be reset, and six are for AVA_VAN vulnerabilities addressed by this release.
- Analytic bug fixes: 92 have no impact and 5 have only minor impact. Of these, one is for usability, one is to prevent future AVA vulnerabilities, and the last three are for AVA_VAN vulnerabilities addressed by this release.

Description of ALC Changes:

1. Security Target – The Security Target has been updated to identify the new hardware models. No other changes were necessary to the Security Target as all changes were minor and did not impact the ST.
2. Guidance document – The Guidance document was updated to identify the new hardware.

Assurance Continuity Maintenance Report:

- GSS submitted an Impact Analysis Report (V1.0), on behalf of Versa Networks to add 7 new hardware models and make a number of software bug fixes.
- Updates consist of bug fixes and enhancements to the operation of the system
- There are no security relevant fixes so no new certification is required.
- No development environment changes occurred that impacted the product.
- There were no changes that required the evaluators to do any additional testing.

Description of Regression Testing:

Versa conducts regression testing for all modifications integrated into the product. This testing approach encompasses both security assessments and functional evaluations. Versa maintains a test suite that is executed on a daily or weekly basis with pass/fail results automatically generated and sent to developers via email. Test suites include sanity tests and full regression tests. Sanity test suites run daily and cover critical functions such as upgrading, service/feature stability, UI regression and smoke tests, and focused tests on new/changed functionality. Sanity tests are performed on daily builds across multiple platforms. Regression test suites include various other performance, stress/endurance, scale, and interoperability test suites. Full regression suites are run weekly and on-demand and must reach certain thresholds defined by the release manager. Once the release has been deemed acceptable by the release manager, the build is published and customers are notified with release notes. Each release candidate is also subjected to a suite of vulnerability and compliance scans, where the release is gated by any critical or high severity security issues found.

Vulnerability Assessment:

The public vulnerability search was updated from the search on 3/28/2024 on 2/27/25. No new public vulnerabilities were discovered that are applicable to the TOE. The evaluator searched the following databases with the 39 terms below.

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)

The evaluator searched the databases listed just above with the 39 terms below

- Versa
- Versa Networks
- Versa Director 22.1
- Versa Operating System 22.1
- VOS 22.1
- Versa SD-WAN Controller 22.1
- Versa SD-WAN Branch 22.1
- Versa Analytics 22.1
- Versa CSG
- Ubuntu 18.0.4.6 LTS
- Bouncy Castle FIPS Java API 1.0.2.3
- Bouncy Castle 1.0.2.3
- Rambus Quicksec 6.1
- Quicksec 6.1
- OpenSSL 1.1.1-1ubuntu2.1~18.04.23
- OpenSSL 1.1.1-1ubuntu2.1
- OpenSSH 8.4p1-2
- Linux kernel 5.4.0
- Linux kernel 4.15.0-1117-fips
- Linux kernel 4.15.0
- Tomcat 9.0.98
- rsyslog 8.32.0-1ubuntu4.2
- rsyslog 8.32.0
- ntp 1:4.2.8p10+dfsg-5ubuntu7.3+esm1
- ntp 1:4.2.8p10 Intel Xeon
- Intel Xeon CPU E5-2683 v4
- Intel Xeon D-2187NT
- Intel Xeon Gold 6252N
- AMD EPYC 7713P
- AMD EPYC
- Intel Xeon Silver 4514Y

- Intel Atom C3758
- Intel Atom C3958
- VMware ESXi 7.0U2
- ESXi 7.0U2
- Dell VEP 4600
- Dell Poweredge R7515
- MetaSwitch
- Intel DPDK 16.04TCPTCP

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on February 27, 2025. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

There have been changes to add hardware platforms to the evaluation. The same software image is used on the new platforms as is used on the evaluated platforms. Minor bug fixes and security patches have been applied. The ST has been updated to reflect the new hardware platforms. The Guidance document was updated to reflect the new hardware platforms.

Based on this and other information from within this IAR document, the assurance impact of these changes is minor.

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 changed to add the new hardware models identified above. The Guidance Document was also updated to add the new hardware models.

Based on this and other information from within this IAR document, the Validation Team agrees that the assurance impact of these changes is minor.