ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Varonis Data Security Platform v8.6.51

Varonis Data Security Platform v8.6.51

Maintenance Report Number: CCEVS-VR-VID11336-2024

Date of Activity: August 12, 2024

References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, 12 September 2016
- Common Criteria, *Assurance Continuity: CCRA Requirements*, Version 2.1, June 2012
- *Varonis Data Security Platform Impact Analysis Report For Common Criteria Assurance Maintenance; Update from Version 8.1 To Version 8.6.51*, version 0.2, August 5, 2024
- *Varonis Data Security Platform v8.6.51 Security Target*, Version 1.3, April 10, 2024
- *Varonis Data Security Platform v8.6.51 Common Criteria Configuration Guide*, Version 1.4, April 9, 2024
- *Vulnerability Assessment for Varonis Data Security Platform (DSP) v8.6.51*, Version 0.5, August 5th, 2024.
- *Protection Profile for Application Software*, Version 1.4, dated, 7 October 2021

Assurance Continuity Maintenance Report:

Acumen Security submitted an Impact Analysis Report (IAR) for the Varonis Data Security Platform, Version 8.6.51 (was Version 8.6) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on August 5, 2024. 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 (ST), the Administrator's Guide (AGD), and the IAR. The ST and AGD were updated to the new version of the TOE.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target:	**Maintained Security Target:**

Varonis Data Security Platform v8.6.51 Security Target, Version 1.2, February 23, 2024	See references above. Updated to identify the new TOE version number and updated AGD version and date.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: Varonis Data Security Platform v8.6.51 Common Criteria Configuration Guide, Version 1.3, February 23, 2023	**Maintained Guidance Documentation:** See references above. Revised to refer to the current product version.
Lifecycle: None	No changes required.
Testing: None	Varonis has performed vulnerability testing, functional regression testing, and unit testing on version 8.6.51. Regression testing is conducted by the quality assurance team within Varonis. The testing executed by the quality assurance team exercises all functionality of the product, including those claimed within the scope of the Common Criteria evaluations.
Vulnerability Assessment: None	The public search was updated on August 5, 2024. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The TOE has been updated from Varonis Data Security Platform, version 8.6 (8.6.22 per the naming standard). To maintain consistency with the Security Target (ST) and the Assurance Guidance Document (AGD), version 8.6 has been referenced as a prior version. Assurance maintenance was carried out for the Varonis Data Security Platform, version 8.6.51. Below is a summary of the changes.

Major Changes

None.

Minor Changes

Twenty-three enhancements were identified in the IAR between versions 8.6.22 and 8.6.51 along with a description and given rationale. The description and rationale for each enhancement was inspected and the overall Minor Change characterization was considered appropriate. None of the

changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary. The following table includes a summary of the changes presented in the IAR. The changes have been categorized according to Enhancements per software version.

Category	Number of Enhancements	Assessment
Version 8.6.32	10	Enhancements were made to: • support new data sources, • the Data Transport Engine view capability, • the ability to receive DNS events, • the creation of domains/servers, • DatAdvantage performance, • shared mailboxes for monitoring, • support for CTERA features, • additional authentication capabilities, • product rebranding, and • removal of support for outdated products. None of the changes resulted in changes to the ST or guidance documentation. The changes were either unrelated to SFRs or outside the scope of the evaluated configuration. Thus, the original testing still holds, and any testing was covered by vendor non-evaluation regression testing.
Version 8.6.41	8	Enhancements were made to • support Department of Defense (DoD) tenants, • support additional synched folder event types, • update DatAlert threat models, APIs, and rules, • updates Data Classification Labels, • update support for Panzua, • to receive additional DNS, VPN, and Proxy events, • require PowerShell for certain capabilities, and • remove support for outdated products. None of the changes resulted in changes to the ST or guidance documentation. The changes were either unrelated to SFRs or outside the scope of the evaluated configuration. Thus, the original testing still holds, and any testing was covered by vendor non-evaluation regression testing.

Version 8.6.51	5	Enhancements were made to • update DatAlert threat models, threat model names/descriptions, and configuration, • update receipt of Proxy events, • update external user sign-in, search capabilities, and add new settings, • updates Data Classification Labels configuration, and • support SQL Server 2022. None of the changes resulted in changes to the ST or guidance documentation. The changes were either unrelated to SFRs or outside the scope of the evaluated configuration. Thus, the original testing still holds, and any testing was covered by vendor non-evaluation regression testing.

Regression Testing:
As noted above, Varonis has performed regression testing on each release. Regression testing performed includes partial automated testing as well as manual test execution by the Quality Assurance Team within Varonis. As part of all product releases, testing includes all vulnerability, regression, and unit testing. Testing covers functionality of the product, including testing in accordance with the Common Criteria requirements to ensure no previous functionality has been impacted.

Equivalency:
The security functionality of the 8.6.51 software update remains the same as the prior evaluated version. The platforms are unchanged from the original evaluation version.

NIST CAVP Certificates:
The same cryptographic modules are used in 8.6.51 and in 8.6. The CAVP certificate numbers referenced during the 8.6 evaluation have not changed.

Vulnerability Analysis:
A new search was performed for vulnerabilities from the time of the original evaluation (February 28, 2023) to August 5, 2024. The search was conducted against the same vulnerability databases and used the same terms as the original evaluation:

- Varonis 8.6
- DatAdvantage
- DataPrivilege
- Varonis Management Console
- Varonis Data Classification Engine
- DatAlert

- Varonis Remediation Engine
- Varonis Data Transfer Engine
- Third party libraries as found in Appendix A of the ST

The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were found.

Conclusion:

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

Regression testing was done and was considered adequate based on the scale and types of changes made. The lab also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, the platforms did not change and there were no necessary alterations to the NIST cryptographic certificates. Therefore, CCEVS agrees that the original assurance is maintained for the product.