CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

NetApp Storage Encryption (NSE) Running ONTAP 9.10.1P14

Maintenance Report Number: CCEVS-VR-VID11174-2023

Date of Activity: 21 September 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." March 20, 2013

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 2.1 June 2012

NetApp Storage Encryption (NSE) Running ONTAP 9.10.1P14 Security Target Version 1.3 21 September 2023

NetApp Storage Encryption (NSE) Appliances Running ONTAP 9.10.1P14 Impact Analysis Report Version 1.1 September 21, 2023

Affected Evidence:

NetApp Storage Encryption (NSE) Running ONTAP 9.10.1P14 Security Target Version 1.3 22 August 2023

Description of ASE Changes:

The changes described in this section constitute all changes made to NetApp Storage Encryption (NSE) appliances running ONTAP 9.10.1P14 since the previous Assurance Continuity Maintenance version (NetApp Storage Encryption (NSE) Appliances running ONTAP 9.10.1P7 Impact Analysis Report).

The code implementing the SFRs is less than 1% of the code implementing the ONTAP operating system. Of the SFR relevant code for NSE (cPP FDE-AA), there were changes in less than 0.1% of that code between the ONTAP 9.10.1P7 and ONTAP 9.10.1P14 patch releases, with none of the changes impacting existing cPP FDE-AA SFRs or AGDs. Changes associated with each patch (P) release from ONTAP 9.10.1P8 through ONTAP 9.10.1P14 are summarized below.

Changes associated with each patch (P) release from ONTAP 9.10.1P8 through ONTAP 9.10.1P14 are summarized below. None of the changes are security relevant and have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE.

1. ONTAP 9.10.1P8 : There are 54 changes with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:
   - For 40 of these changes, the "issue does not impact the TSF or SFRs associated with the TOE".
   - For 7 of these changes, the "bug fixes do not affect the security functionality of the TOE nor change the ST or guidance documentation and has no effect on the result of any Assurance Activity test".
   - For 1 change, the TSF interfaces are not affected.
   - For 11 of the changes, the Evaluated configuration does not allow for Metro Cluster, administration via the REST interface, ZAPI or ONTAP.
   - There is 1 change to address a CVEs; which is also listed as not impacting the TSF or SFRs associated with the TOE.
2. ONTAP 9.10.1P9: There are 40 with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:
   - For 34 of these changes, the "issue does not impact the TSF or SFRs associated with the TOE".
   - For 2 changes, the "bug fixes do not affect the security functionality of the TOE nor change the ST or guidance documentation and has no effect on the result of any Assurance Activity test".
   - For 4 changes, the Evaluated configuration does not allow for Metro Cluster, administration via the REST interface, ZAPI or ONTAP.
   - For 2, the changes are to address CVEs.
   - 5 of the changes not impacting the SFRs are also counted in other categories.
3. ONTAP 9.10.1P10: There are 51 changes with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:
   - For 25 of these changes, the "issue does not impact the TSF or SFRs associated with the TOE".
   - For 13 changes the "bug fixes do not affect the security functionality of the TOE nor change the ST or guidance documentation and has no effect on the result of any Assurance Activity test".
   - For 13 changes, the Evaluated configuration does not allow for Metro Cluster, administration via the REST interface, ZAPI or ONTAP.
   - For 1, the changes are to address CVEs.

- 1 of the changes non-AGD changes also is counted in the Not allowed in the Evaluated Configuration.

4. ONTAP 9.10.1P11: There are 41 changes with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:
   - For 32 of these changes the IAR states that the "issue does not impact the TSF or SFRs associated with the TOE.
   - For 6, the Evaluated configuration does not allow for Cloud Volumes ONTAP (CVO) or administration via the REST interface.
   - There are 4 changes to address CVEs; one of these is also listed as not impacting the TSF or SFRs associated with the TOE.
5. ONTAP 9.10.1P12: There are 57 changes with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:
   - For 38 of the changes, the "issue does not impact the TSF or SFRs associated with the TOE".
   - For 16 the "bug fixes do not affect the security functionality of the TOE nor change the ST or guidance documentation and has no effect on the result of any Assurance Activity test".
   - For 3, the Evaluated configuration does not allow for Metro Cluster, administration via the REST interface, ZAPI or ONTAP.
   - For 3, the changes are to address CVEs.
   - 3 of the changes are counted in more than 1 category.
6. ONTAP 9.10.1P13: There are 50 changes with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:
   - For 39 of the changes, the "issue does not impact the TSF or SFRs associated with the TOE".
   - For 4 changes, the "bug fixes do not affect the security functionality of the TOE nor change the ST or guidance documentation and has no effect on the result of any Assurance Activity test".
   - For 4 changes, the Evaluated configuration does not allow for Metro Cluster, administration via the REST interface, ZAPI or ONTAP.
   - For 4, the changes are to address CVEs.
   - 2 of the changes are counted in more than 1 category.
7. ONTAP 9.10.1P14: There are 39 changes with this patch (P) release. None of the changes were considered Security Relevant and all were deemed to have only minor impact. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE. The Supporting Rationale described here:

- For 39 of the changes, the "issue does not impact the TSF or SFRs associated with the TOE".
- For 5, the changes are to address CVEs.
- The 5 changes for CVEs also do not impact the SFRs.

Affected Developer Evidence:

Items associated with this section have been included in the previous section, **Error! Reference source not found.**.

Description of ALC Changes:

Changes to the Security Target revision were made, going from version 1.2 (14 September 2022) to 1.3 (21 September 2023) with the update of the TOE software version. No other documentation was affected.

Changes to the Developer Evidence:

- **TSF Interfaces:** No changes to TSF Interfaces – There is no difference in the mapping of the SFRs to interfaces and no additional testing is required. Tests from the previous evaluation will be covered in the regression testing.
- **TSF Platform (TOE Hardware):** No new components were added.
- **SFRs:** There have no changes to the SFRs identified in the ST.
- **New Security Functions:** No new security features have been added.
- **Assumptions and Objectives:** No changes to assumptions and objectives.
- **Assurance Documents:**
    - AVA changes – Vulnerability searches were conducted to ensure the TOE is free of vulnerabilities.
    - ASE Changes – The ST was updated to reflect the new version of the TOE.
- **Changes** – There were multiple changes in going from ONTAP 9.10.1P7 to ONTAP 9.10.1P14; the impact of these changes is summarized above. None of the changes had any impact on the AGD, SFRs, the Security Target or the TOE.
- **TOE Environment** – There were no changes to the TOE Environment.

Assurance Continuity Maintenance Report:

- NetApp submitted “NetApp Storage Encryption (NSE) Appliances Running ONTAP 9.10.1P14 Impact Analysis Report Version 1.1 September 21, 2023” an Impact Analysis Report (IAR) on behalf of NetApp, Inc.
- The Impact Analysis Report (IAR) documents all changes made to the NetApp Storage Encryption (NSE) Appliances running ONTAP 9.10.1P14 since the previous Common Criteria evaluation (CCEVS-VR-VID11174-2022).

- The IAR indicates that the impact of all the individual changes is minor, so it concludes that the sum of all the changes to the TOE have only minor impact.
- Changes to the Security Target are detailed in the table above.
- All TOE cryptographic services are provided by the NetApp software modules CryptoMod version 2.2 and the NetApp Cryptographic Security Module (NCSM). The product updates had no effect on the CAVP certificates. The cryptographic primitives have not been affected by the product updates and the CAVP certificates remain valid for the 9.10.1P14 evaluation.

Description of Regression Testing:

NetApp followings a "continuous integration testing" (CIT) model for all submitted code branch changes in addition to performing extensive automated regression (functional hardening "BOTs" aka FHBOT) and non-automated, free form, "try to break the system", testing prior to every major or minor (patch) ONTAP release.

Vulnerability Assessment:

A public search for new vulnerabilities that might affect the TOE since the last IAR analysis (September 29, 2022) was performed. In summary, all publicly disclosed security vulnerabilities applicable to TOE versions prior to this version have been mitigated.

A search of the NVD database (https://nvd.nist.gov/vuln/search) using "Clustered Data ONTAP" as the search term (exact match), performed on **September 21, 2023**, produced a total of 37 records with 1 record that was published after the last IAR analysis (September 29, 2022).

A search of the NVD database (https://nvd.nist.gov/vuln/search) using "NetApp" as the search term (exact match), performed on **September 21, 2023**, produced a total of 79 records with 1 record that was published after the last IAR analysis (September 29, 2022). That record (CVE-2023-27311) is for a separate NetApp product (BlueXP), not the TOE.

A search of the NVD database (https://nvd.nist.gov/vuln/search) using "ONTAP" as the search term (exact match), performed on **September 21, 2023**, produced a total of 60 records with 1 record that was published after the last IAR analysis (September 29, 2022). That record (CVE-2022-23241) is the same as that in Table 12.

A search of the NetApp database (https://security.netapp.com/advisory/) using "Clustered Data ONTAP" as the web page search term (example: Ctrl-F or Command-F), performed on **September 21, 2023,** produced a total of 5537 records with 1 record that was published after the last IAR analysis (September 29, 2022).

Vendor Conclusion:

Since all changes made between the last validated version (ONTAP 9.10.1P7) and ONTAP 9.10.1P14 did not impact any of the TOE SFRs or SARs, and since there was no need to modify any of the Common Criteria maintained guidance for the TOE, NetApp's conclusion is the assurance impact is minor.

Validation Team Conclusion:

The Validation team has reviewed the changes and concurs that the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cider version of this product.