ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Red Hat Certificate System

---

Red Hat Certificate System 9.4 batch update 3

Maintenance Report Number: CCEVS-VR-VID10831-2021

Date of Activity: 31 March 2021

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008
- Red Hat Certificate System Analysis Report (IAR), Red Hat, Version 1.1, 31 March 2021
- Protection Profile for Certification Authorities Version 2.1 (PP_CA_21)

Documentation reported as being updated:

- Security Target:
  - Red Hat Certificate System (CAPP21) Security Target, version 1.1, February 12, 2021
- Red Hat Certificate System 9 Guidance:
  - Administration Guide (Common Criteria Edition), Revision 9.4-1, February 2021
  - Planning, Installation, and Deployment Guide (Common Criteria Edition), Revision 9.4-1, February 2021

Assurance Continuity Maintenance Report:

The Red Hat Corporation has prepared and submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 31 March 2021. An 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 2.0.

The purpose of this Assurance Continuity Maintenance Report (ACMR) is to summarize and present the findings of CCEVS' analysis of the IAR and associated evidence submitted in support of the changes to the original evaluation, and to make a determination regarding the appropriateness of Assurance Maintenance Continuity for the evaluation.

Introduction:

The evaluation, VID10831, was conducted by Gossamer Laboratories. The product met the security requirements specified by the NIAP approved protection profiles:

- Protection Profile for Certification Authorities Version 2.1

Red Hat, Inc has requested an assurance maintenance activity for the product to update the original evaluation and changes to the original product are detailed in the IAR.

Summary Description:

The only differences in the TOE software were the application of security patches. No changes were made to the TOE hardware. The documentation has been updated to reflect the software update version, the Security Target, Administration Guide and Planning, Installation and Deployment Guide.

TOE new features:

Feature	Description
N/A	No new features were added.

TOE changes to existing functionality:

Feature	Description
N/A	No changes to TOE

TOE security patches:

Security patches were applied to the TOE and they are the only reported changes to the TOE. The patches addressed publicly reported vulnerabilities and defects. The security updates were found to have no impact to the security functionality of the TOE.

The following table provides a brief description of the security patches and the concerned CVEs.

CVE	Description of change
CVE-2019-10180: A vulnerability was found in all pki-core 10.x.x version, where the Token Processing Service (TPS) did not properly sanitize several parameters stored for the tokens, possibly resulting in a Stored Cross Site Scripting (XSS) vulnerability.	Added input validation for TPS
CVE-2020-1696: A flaw was found in the all pki-core 10.x.x versions, where Token Processing Service (TPS) where it did not properly sanitize Profile IDs, enabling a Stored Cross-Site Scripting (XSS) vulnerability when the profile ID is printed.	Same fix in CVE-2019-10180 addressed this issue
CVE-2019-10221: A Reflected Cross Site Scripting vulnerability was found in all pki-core 10.x.x versions, where the pki-ca module from the pki-core server.	Sanitized the Server generated error message to escape the HTML tags with URLs if any present
CVE-2019-10179: A vulnerability was found in all pki-core 10.x.x versions, where the Key Recovery Authority (KRA) Agent Service did not properly sanitize recovery request search page, enabling a Reflected Cross Site Scripting (XSS) vulnerability.	Same fix in CVE-2019-10180 addressed this issue
CVE-2019-10146: A Reflected Cross Site Scripting flaw was found in all pki-core 10.x.x versions module from the pki-core server due	The XSS is addressed in PathLength attribute in CA agent web page - The input type is set to number when "integer" is encountered

to the CA Agent Service not properly sanitizing the certificate request page.	- The server error message is html escaped, before it gets displayed in client browser
CVE-2019-17007: In Network Security Services before 3.44, a malformed Netscape Certificate Sequence can cause NSS to crash, resulting in a denial of service.	Add a check that we decode a certificate sequence correctly before actually using it. Any anomalies in the cert sequence are reported as errors
CVE-2019-17006: In Network Security Services (NSS) before 3.46, several cryptographic primitives had missing length checks.	Added additional length checks around cryptographic primitives to make sure each primitive affected receives sane input values, adhering to rfc specs. If errors are detected, abort the given operation with an error

Regression Testing:

Regression testing was performed on the security patched TOE. The testing was performed by the vendor's quality assurance engineering team and consisted of manual and automated testing. All tests were satisfied and passed.

Vulnerability Analysis:

An updated search for vulnerabilities was performed, on the updated TOE, February 15, 2021. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were detected.

The following search terms were used in the updated vulnerability analysis:

- RHCS
- RHEL
- Thales
- nShield
- Certificate Authority
- NSS
- tomcat
- TLS
- dogtag
- pki-core

Conclusion:

CCEVS reviewed the description of the changes which consisted of the required security patches. There were no changes to the TSF interfaces, SFRs, or security functions introduced by the TOE patches. All of the changes were considered to be minor in impact. In addition, the existing NIST CAVP certifications were also not impacted by any of the changes.

The CCTL also reported that there were no vulnerabilities associated with any of the models. Therefore, CCEVS agrees that the original assurance is maintained for the product.