ASSURANCE CONTINUITY MAINTENANCE REPORT FOR: Red Hat® Certificate System 10.4.4

Maintenance Update of Red Hat® Certificate System 10.4

Maintenance Report Number: CCEVS-VR-VID11468-2026

Date of Activity: 13 August 2026

References:

- Common Criteria "Assurance Continuity: CCRA Requirements", version 3.1, February 2024.
- National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme Publication #6 Assurance Continuity: Guidance for Maintenance and Re-evaluation, v3.0, 12 September 2016
- Impact Analysis Report for Red Hat® Certificate System 10.4, Version 1.0, 22 July 2026
- Red Hat® Certificate System 10.4.4 Security Target, Version 0.7, 22 July 2026
- Red Hat Certificate System 10 Administration Guide (Common Criteria Edition – Assurance Maintenance), 23 July 2026
- Red Hat Certificate System 10 Planning, Installation, and Deployment Guide (Common Criteria Edition - Assurance Maintenance), 23 July 2026
- Protection Profile for Certification Authorities, Version 2.1, 01 December 2017

Documentation Updated:

- **Security Target:** Red Hat® Certificate System 10.4.4 Security Target, Version 0.7, 22 July 2026
  - Changes in the maintained ST are:
    - Updated identification, date and version of the ST
    - Section 1 - Updated TOE software version
    - Section 1.4.2 – Updated AGD documentation to latest versions
- **Supplemental Guide**: Red Hat Certificate System 10 Planning, Installation, and Deployment Guide (Common Criteria Edition -Assurance Maintenance), August 4, 2026
  - Changes in the maintained Guidance are:
    - Updated title from: "Red Hat Certificate System 10.4 Planning, Installation, and Deployment Guide (Common Criteria Edition)" to "Red Hat Certificate System 10 Planning, Installation, and Deployment Guide (Common Criteria Edition - Assurance Maintenance)"
    - Updated TOE version from v10.4 to v10.4.4
    - Updated document date to August 4, 2026

- **Administration Guide**: Red Hat Certificate System 10 Administration Guide (Common Criteria Edition -Assurance Maintenance), August 4, 2026
    - Changes in the maintained Guidance are:
        - Updated title from "Red Hat Certificate System 10.4 Administration Guide (Common Criteria Edition)" to "Red Hat Certificate System 10 Administration Guide (Common Criteria Edition)"
        - Updated TOE version from v10.4 to v10.4.4
        - Updated document date to August 4, 2026

Assurance Continuity Maintenance Report:

Gossamer Security Solutions submitted an Impact Analysis Report (IAR) on behalf of Red Hat Inc. and the Red Hat Certificate System 10.4.4 to CCEVS for approval in July 2026. The IAR is intended to satisfy requirements outlined in Common Criteria document "Assurance Continuity: CCRA Requirements", version 3.1, February 2024. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result 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, the Supplemental Configuration Guide, and the Impact Analysis Report (IAR).

Changes to TOE:

The TOE changes consist of updating the TOE software from version 10.4 to 10.4.4. The software updates include new non-security relevant features and bug fixes.

Summary of feature updates:

- Changes to how serial numbers for certificates are generated and handled. This is an accounting mechanism and not security related.
- Changes to features that are outside the scope of the original evaluation.

Summary of bug fixes:

- CVE-2023-4727 patched.

Regression Testing:

Regression testing by the Red Hat Certificate System Engineering Team was performed on the updated TOE software utilizing the Errata Tool Workflow. Errata Tool (ET) is an internal capability designed to provide quality control of Red Hat software as a part of the product release pipeline. It is integrated with internal software security tracking to help ensure compliance with patching and bug fixes. The IAR documents the ET workflow and describes how test evidence is developed and reviewed by the Red Hat engineering and security team(s) before updates are released into production software.

Vulnerability Assessment:

The evaluation team conducted new vulnerability searches in support of this ACMR. The most recent search was conducted on July 23, 2026, and used the following sources:

- https://nvd.nist.gov/vuln/search
- https://www.cve.org/
- https://www.cvedetails.com/vulnerability-search.php
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Search terms and keywords were relevant to the TOE and TSF functionality and are documented in the Impact Analysis Report for Red Hat® Certificate System 10.4. The terms are not reproduced here.

No open vulnerabilities applicable to the TOE were identified.

Conclusion:

The specific changes identified in this ACMR to the product are considered minor and do not affect the security claims in the Red Hat Certificate System 10.4.4 Security Target. There were no changes to SFRs, Security Functions, Assumptions or Objectives. The security target and the Common Criteria Evaluation Guidance Documents were updated to reflect the version changes of the TOE.

Regression test results were declared by the evaluation security team to be consistent with the previous test results. The evaluation security team searched the public domain for any new potential vulnerabilities that may have been identified since the evaluation completed. The search did not identify any new potential vulnerability.

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.