ASSURANCE CONTINUITY MAINTENANCE REPORT FOR SailPoint IdentityIQ v8.3p2

SailPoint IdentityIQ

Maintenance Report Number: CCEVS-VR-VID11043-2023

Date of Activity: April 18, 2023

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- SailPoint IdentityIQ v8.3p2 Common Criteria Security Target, ST Version 1.2, 31 March 2023
- Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013

Assurance Continuity Maintenance Report:

SailPoint submitted an Impact Analysis Report (IAR) for the "SailPoint IdentityIQ v8.3p2" to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 3 April 2023. 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 IAR was prepared by the Booz Allen Hamilton Cyber Assurance Testing Laboratory on behalf of SailPoint. The evaluation evidence submitted for consideration consisted of the Security Target (ST), updated Guidance Documentation described further in the table below, the Impact Analysis Report (IAR), and release notes.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Impact Analysis Report: SailPoint IdentityIQ Version 8.3p2 Impact Analysis Report (IAR) Version 1.0 March 31, 2023	**Evaluation Evidence:** New – summarized the old TOE, new TOE, provides an explanation of the changes and rationale of why the changes are sufficiently minor to claim the original evaluation's work still applies sufficiently.
Security Target: SailPoint IdentityIQ v8.3p2 Common Criteria Security Target, Version 1.2, March 31, 2023	**The ST was updated to include:** The Security Target document was updated to be applicable to the updated versions of the TOE for version 8.3p2: o SailPoint IdentityIQ v8.3p2 Common Criteria Security Target v1.2 dated March 31, 2023. Updates include: ▪ Identification of the Changed TOE version ▪ Security Target dates and versioning ▪ References to Changed TOE guidance documentation ▪ The excluded from the evaluated configuration list ▪ Reference to the latest version of the Chrome web browser
Guidance: SailPoint IdentityIQ System Configuration version 8.3p2	**The Guidance Document** – The guidance document was updated to be applicable to the updated versions of the TOE for versions 8.3p2: o SailPoint IdentityIQ v8.3p2 Supplemental Administrative Guidance v1.3 dated March 31, 2023 ▪ Identification of the Changed TOE version ▪ Update of document dates and versioning ▪ Update of references to Changed TOE Security Target and other guidance documentation ▪ Update the reference to the latest version of the Chrome web browser
Release Notes	Release Notes • The release notes were created for each patch between the Validated TOE (version 8.2p2) and the Changed TOE (version 8.3p2). They contain a listing of the new features implemented and bug fixes provided by these patches.

Changes to the TOE:

Each of the changes to "SailPoint IdentityIQ v8.3p2" was analyzed to determine whether it fell into the categorization of "Major Changes" or "Minor Changes". The conclusion was that all of the changes were minor and had either minor or no impact on the evaluated product.

New Features

The IAR New Features Section contains two tables, "New Features for SailPoint IdentityIQ 8.3p2" and "Connector Enhancements for SailPoint IdentityIQ 8.3p2". These tables summarize the new features that have been added for all releases between the Validated TOE and the Changed TOE along with a brief description of each feature. A brief summary of the seven new features is provided below. The changes to the Connector features are also summarized below. There were two sets of additions and two removals or deprecations. The IAR states that the new features were found to have no impact in areas of validated functionality and that the vendor demonstrated that these new features were properly implemented by providing evidence of regression testing which also demonstrated that these new features do not have adverse effects on the behavior of the TSF. The IAR further specifies that there are no changes that modify the implementation of SFRs, remove the enforcement of existing SFRs, or force the addition of any security-relevant functionality or interfaces. The IAR states that none of the changes impacted the ST, ADV, ATE or AGD.

New Features for SailPoint IdentityIQ 8.3p2

1. Notifications in Microsoft Teams
    - Allows notifications from IdentityIQ to be delivered directly to users as notifications in their Microsoft Teams environment
2. Role Management & Analysis
    - Allows roles to be filtered based on details of the entitlements included directly in their profiles, or in the profiles of other roles with a required/permitted/inherited relationship
3. Flagging Elevated Access in Roles and Entitlements
    - Permits classification of roles and entitlements as allowing Elevated Access
4. Active Directory Native Move/Rename Support
    - Adds support for detecting when changes are made to an account or a groups DN in Active Directory and ensuring this identity data is updated in all locations where the DN was referenced
5. AI Recommendations for Roles
    - Allows IdentityIQ users to use the AI Services to get deeper insight and recommendations for the actions related to roles such as access reviews and access request approvals
6. SAML Authentication for e-Signatures
    - Allows the user to perform electronic signatures with the SAML-based SSO feature being enabled
7. OAuth 2.0 Authentication for Email
    - Adds support for OAuth2 authentication protocol for sending email notifications

Connector Enhancements for SailPoint IdentityIQ 8.3p2

1. New Connectors

- New out-of-the-box connectors for the following enterprise applications, which simplifies the connectivity of these systems: MEDITECH; BMC Helix ITSM Service Desk

2. Enhancements to Non-Evaluated Connectors
   - Allows for IdentityIQ to integrate with third-party enterprise applications for its primary purpose
3. Connectivity Dropped Platform Support
   - Support dropped for connectors to older versions of the enterprise applications previously used to connect with: Linux Connector; SailPoint Identity Governance Connector for ServiceNow; ServiceNow Service Desk Integration Module
4. Dropped/Deprecated Connector Support
   - Support dropped/deprecated for connectors to older versions of the enterprise applications previously used to connect with: Yammer Connector

Bug Fixes

The vendor provided a summary of the bug fixes. The 15 categories are summarized below. While there were a number of these fixes, none were identified in security-relevant behavior during initial validation testing. Most of the bug fixes were not considered to be security relevant because they represent changes to functionality that was not included as part of the TSF or were considered to be general performance/diagnostic/stability issues that were unrelated to security. Other bug fixes applied to issues that were at a lower level of detail than what was tested. In general, these bug fixes did not change how the TSF are performed, so much as they allow the TOE to continue to implement the TSF in a manner that is consistent with what the Security Target defines. None of the bug fixes impacted the ST, ADV, ATE or AGD.

Bug Fix Categories

1. Active Directory Connector (50)
2. Non-Evaluated Connectors (No count provided)
3. Alerts/Notifications (25)
4. AI Services (12)
5. IdentityIQ File Access Manager (FAM) (13)
6. Cloud Access Management Module (8)
7. Privileged Account Management Module (8)
8. Applications (23)
9. Audit (5)
10. Database (8)
11. Active Directory Compliance Checks (29)
12. Excluded Functionality and Operational Environment Components (9)
13. GUI/Grammatical Fix (141)
14. Unevaluated Authentication (4)
15. Performance (146)
16. Managed Roles (18)
17. Vulnerabilities (83)
18. Workflow (24)

TOE Environment

There were changes to the operational environment of the TOE; these include changes to the supported Operating Systems, Application Servers, Databases, Java Platforms, and Cloud Platforms. The list of each of these is contained in the ST. The IAR stated that because these changes were

reviewed and found to not be significant, it was concluded that they imposed “minor impact” to the overall evaluation. The IAR specified that Regression testing was performed by the vendor using the changed environment. The Evaluator reviewed the results and determined that they were consistent with the validated results from the previous evaluation. For the Database Servers and Cloud Platforms, the IAR states that none of the changes impacted the ST, ADV, ATE or AGD. For Operating Systems, Application Servers, and Java Platforms the IAR states that there was no impact to ST other than the list of excluded environments has been updated in Section 2.4.1 ‘Excluded from the Evaluated Configuration’ of the ST for clarity. The ADV, ATE or AGD for these environments were not impacted.

Note that the current list of supported Operating Systems is limited to the following:

- Windows Server 2022 & 2019
- Solaris 11 & 10
- IBM AIX 7.3 and 7.2
- Red Hat Linux 8.5
- SuSe Linux 15

Regression Testing:

SailPoint performs continuous testing on IdentityIQ's code with testing cycles occurring multiple times a day and ensures that each piece of updated code is tested several times before a new image is released. Any time a bug is fixed, or a new feature is implemented in IdentityIQ, the new code is unit tested to ensure that it operates correctly. The code will then be merged with the base code where SailPoint's Quality Assurance System performs a full suite of unit tests and operational tests to verify that the code changes were properly implemented and do not impact any of IdentityIQ's other functionality. Included in the operational tests are test cases that were performed during the Common Criteria certification of SailPoint IdentityIQ version 8.2p2 (Validated TOE). Once SailPoint is ready to release a new software image, SailPoint will create a build of the software for the release which is also tested using SailPoint's Quality Assurance System. The unit tests and operational tests that comprise the Quality Assurance System are maintained by SailPoint's developers and Quality Assurance team to ensure that tests are updated to test the latest code.

SailPoint performed regression testing on SailPoint IdentityIQ version 8.3p2 (Changed TOE) and determined that the behavior of the TSF remained consistent with the testing during the original evaluation. This consistency confirms that the new features and bug fixes described in Section 3 had no effect on any security-related functionality of the TOE.

NIST CAVP Certificates:

This evaluation does not claim any FCS requirements as all of the cryptographic functions are performed by the underlying platform. Therefore, no NIST CAVP Certificate is directly linked to this product.

Vulnerability Analysis:

The lab defined keywords to perform a public search for vulnerabilities. The keywords are defined based on the vendor's name, product (TOEs) name, general technology product terms, and libraries compiled with the TOE. A public search for vulnerabilities that might affect the TOE was performed on 03/31/2023. All applicable findings must be resolved to pass.

The following public sources were searched during this analysis:

a) NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
b) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
c) US-CERT: http://www.kb.cert.org/vuls/html/search
d) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
e) Offensive Security Exploit Database: https://www.exploit-db.com/
f) Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The following keywords were used individually and as part of various permutations and combinations to search for vulnerabilities identified in the public domain:

Keyword	Description
SailPoint	This is a generic term for searching for known SailPoint IdentityIQ vulnerabilities.
IdentityIQ	This is a generic term for searching for known SailPoint IdentityIQ vulnerabilities.
Generic Technology Type	
Identity Credential Management	This is a generic term for searching for known technology type vulnerabilities.
ICM	This is a generic term for searching for known technology type vulnerabilities.
Libraries	
Apache Axis 1.4	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache Axis2 1.7.8	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache bcel 6.5.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache Commons Collections 4 4.4	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache commons io 2.7	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache Commons lang3 3.10	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache commons pool2 2.8.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache commons TEXT 1.10.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache Geronimo 1.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache HttpComponents 4.5.13	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache Log4j 2.17.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache Taglibs 1.2	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.

Keyword	Description
Apache velocity 2.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache: velocity engine core 2.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache: Wink 1.1.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Apache WSS4J 1.6.19	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
AWS SDK For Java Bundle 1.11.354	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Fasterxml Jackson Annotations 2.12.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Fasterxml Jackson Core 2.12.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Fasterxml Jackson Databind 2.12.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Fasterxml Jackson Datatype 2.12.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Annotations 1.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Beanutils 1.9.4	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Codec 1.3 (ITIM integration)	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Codec 1.15	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Collections 3.2	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects DBCP 2 2.7	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Digester 2.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects EL 1.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects FileUpload 1.4	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects IO 2.7	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Javaflow 1.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Lang 2.6	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Lang3 3.10	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Logging 1.2	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Net 3.8	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Pool2 2.8.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Text 1.9	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Eclipse Jakarta Commons Projects Validator 1.7	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.

Keyword	Description
Eclipse Jakarta ORO 2.0.8	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Fusesource Jansi 1.18	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Google Data 1.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Google Guava 30.1-jre	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Google Guava Failureaccess 1.0.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Google Guice 5.0.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Google Guice Servlet 4.2.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Google Gson 2.9.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
JAvax cache api 1.1.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Jodah failsafe 2.0.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Joda.org joda time 2.10.6	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
JQUERY 3.5.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Json Smart 1.2 - ASM Based Accessors Helper	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
JSON PATH 2.4.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
JSON Small and Fast Parser 2.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
JSON Web Token Support For The JVM 0.9.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Lucene 8.8.2	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Squareup Okhttp 2.7.5	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
OWASP Java HTML Sanitizer 20212028.2	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
p6spy 3.9.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
PrimeTEK Primefaces 8.0.12	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Shibboleth Opensaml 3.4.5	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
SmallRye Jandex 2.1.3 Final	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Square Okio 1.15.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Stax 1.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Twilio Project Twilio 8.14.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.

There were no open or unpatched known vulnerabilities to the TOE, nor the libraries used by the TOE, as a result of the public search. Therefore, there are currently no publicly known vulnerability issues that could affect the security posture of a deployed TOE.

The validators confirmed that the vendor assessment determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE.

Conclusion:

As documented in the IAR, there has been added functionalities and bug fixes between the Validated TOE (SailPoint IdentityIQ v8.2p2) to the Changed TOE (SailPoint IdentityIQ v8.3p2). A few of these updates improved the product's functionality related to the TSF by addressing security vulnerabilities, increasing performance, and addressing bugs that caused usability issues. However, most of these updates addressed functionality that was outside the scope of the evaluated configuration. The development evidence (Security Target and Supplemental Administrative Guidance) for the Validated TOE received minor updates to address the Changed TOE to include product and document version updates.

These new features and bug fixes did not impact the ability of the TOE to continue enforcing the security requirements as described by the Validated TOE's Security Target. Furthermore, the methods used to perform functions on the Validated TOE are still available to be used in the Changed TOE, since all updates made to the Changed TOE were done to allow for backwards compatibility to already configured SailPoint IdentityIQ instances. This was also verified through the completion of the regression testing that confirmed the functionality still operated as expected.

Based upon the findings in the IAR and the reasoning provided above in this document, it has been determined that the changes from the validated TOE (SailPoint IdentityIQ v8.2p2) to the Changed TOE (SailPoint IdentityIQ v8.3p2) are of "minor impact".

The overall impact is minor. This is based on the above rationale that new non-security relevant changes and the update of the TOE to SailPoint IdentityIQ v8.3p2 had no impact on the certified TOE.

In addition, a search for vulnerabilities identified none directly affecting the TOE

Therefore, CCEVS agrees that the original assurance is maintained for the product.