ASSURANCE CONTINUITY MAINTENANCE REPORT FOR SailPoint IdentityIQ v8.2p2

SailPoint IdentityIQ

Maintenance Report Number: CCEVS-VR-VID11043-2022

Date of Activity: 04 May 2022

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 v8.2p2 Common Criteria Security Target, ST Version 1.1, 1 April 2022
- 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 v8.2p2" to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 7 April 2022. 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), update Guidance Documentaton described further in the table below, the Impact Analysis Report (IAR), a spreadsheet that provided a categorization of the changes and the associated impact, and further detailed evidence supporting the vulnerability analysis described in the IAR. There number of Guidance Documents increased from the original evaluation because the vendor divided the document into multiple volumes and added new volumes for some of the new features that are outside the scope of the evaluation..

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Impact Analysis Report: SailPoint_IdentityIQ_IAR_v1.0_04072022	**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 v8.2p2 Common Criteria Security Target, Version 1.1, April 1, 2022	**The ST was updated to include:** Security Target – The Security Target document was updated to be applicable to the updated versions of the TOE for version 8.2p2: • SailPoint IdentityIQ v8.2p2 Common Criteria Security Target v1.1 dated April 1, 2022. Updates include: o Identification of the Changed TOE version o Security Target dates and versioning o References to Changed TOE guidance documentation o The excluded from the evaluated configuration list o The Technical Decision Table o Reference to the latest version of the Chrome web browser o Minor grammatical fixes
Guidance: SailPoint IdentityIQ System Configuration version 8.2	**The guidance document was updated to be applicable to the updated versions of the TOE for versions 8.2p2:** Updated – Use System Setup to configure the different options for IdentityIQ.
SailPoint IdentityIQ Lifecycle Manager version 8.2	New – Lifecycle Configuration used to customize the availability of tools and functionality based on end user needs.
SailPoint IdentityIQ Active Directory Connector version 8.2	Updated – The TOE has the ability to communicate with Active Directory to define identity and credential data for enterprise users. This communication is accomplished through the use of connectors. In the evaluated configuration, IdentityIQ will communicate with one or more instances of Active Directory utilizing the ADSI connector. The TOE will also communicate with the Oracle 19c database using JDBC.
SailPoint IdentityIQ Installation Guide version 8.2	Updated – Used to install and deploy SailPoint IdentityIQ on application server. After IdentityIQ is deployed it must be configured to work within the enterprise.
SailPoint IdentityIQ Tasks version 8.2	New –Used to automate the processes which build, update, and maintain the information contained within IdentityIQ.

SailPoint IdentityIQ Password Management version 8.2	New – IdentityIQ supports multiple login configurations, including single sign-on, pass-through authentication, and validation against IdentityIQ's internally stored passwords. Pass-through authentication and internal passwords can be managed through the IdentityIQ user interface
SailPoint IdentityIQ v8.2p2 Supplemental Administrative Guidance, version 1.1, April 1, 2022	New – 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 • Minor grammatical fixes

Changes to the TOE:

Each of the changes to "SailPoint IdentityIQ v8.2p2" 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.:

The TOE was revised with the following changes SailPoint IdentityIQ v8.2p2.

1 Hardware changes – none

2 Changes to the operating environment: The database used in the environment for the evaluated configuration has changed from Oracle 18c to Oracle 19c. The overall list of product supported databases and cloud platforms has also changed, but Oracle 19c is the only one relevant to the evaluated configuration. Regression testing has been conducted by the vendor with the TOE using Oracle 19c as its remote database. These results were reviewed, and it was determined that the results were consistent with the previous validated TOE

3 New features. Most of the new features were for functionality that are excluded from the evaluated configuration and have no impact on the TOE. For the new features with minor security impacts, the vendor has demonstrated that these new features are properly implemented by providing evidence of regression testing to demonstrate that the new features will not have adversely affected the behavior of the TSF.

4 Changes to features that are not part of the evaluated configuration. Those changes did not impact the evaluated configuration.

5 Changes to connectors: There were changes to many of the connectors and connectors to products that were deprecated were removed. The only connector that is relevant to the evaluated configuration is the Active Director connector. The changes to the connector for Active Directory were shown to be for usage outside the scope of the evaluation and to not impact evaluated behaviour of the TOE.

6 Changes for Active Directory: The changes for Active Director were explicitly identified as a separate category but were mostly related to new capabilities that are not part of the evaluated configuration. These were feature additions and modification that had minor impact or no impact.

7 Bug fixes:The vendor provided a summary of the bug fixes. While there were numerous bug fixes, none of those bugs 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; more precisely they allow the TOE to continue to implement the TSF in a manner that is consistent with what the Security Target.. There were some bug fixes for vulnerabilities that were identified after the original evaluation and were fixed for this updated version of the product. Among those potential vulnerabilities the only ones that would have been visible in a vulnerability search of the standard databases were found to be in third party libraries and were fixed by updating to a new version of the library. Since the TOE only relies on the behavior of those libraries at the interfaces and those were not changed, the impact on the TOE for each of the vulnerability fixes was minor

.

Regression Testing:

SailPoint performed regression testing on SailPoint IdentityIQ version 8.2p2 (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 had no effect on any security-related functionality of the TOE.

SailPoint's internal security team performed regression testing including, but not limited to, the following:

- Active Directory Enhancement 10 – regression testing conducted by the vendor with pass-through authentication using Active Directory.
- Regression testing on Edit Preferences page that was changed to be 508/WCAG Compliant
- Active Directory Connector - These bug fixes resolved functionality issues within the Active Directory Connector that SailPoint IdentityIQ supports. This connector was used in the evaluation for the connection between SailPoint IdentityIQ and the Active Directory entities residing in the operational environment when performing management of identities.
- TOE Environment regression testing was performed by the vendor using the changed environment.
- Operating Systems - Regression testing conducted by the vendor with the TOE installed on a server with the Microsoft Windows Server 2016 operating system. The overall list of supported operating systems changed.
- Application Server - Regression testing was conducted by the vendor with the TOE installed on a server using Apache Tomcat 9.0. Changes to the supported application servers list does not impact the ST.
- Database - IdentityIQ no longer supports the use of Oracle 18c database and instead the operational environment component for the database has been updated to Oracle 19c. Regression testing was conducted by the vendor with the TOE using Oracle 19c as its remote database.

The IAR stated that all tests completed satisfactorily.

NIST CAVP Certificates:

There were not changes needed in the NIST CAVP Certificates.

Vulnerability Analysis:

A public search for vulnerabilities that might affect the TOE was performed on 04/06/2022.

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. In the case of the libraries, only the library name was used in the search of the databases. The results from those library searches were then reviewed using the version of the library to eliminate hits that were not applicable to the installed version.:

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	
bcel 6.5.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
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.
commons collections4 4.4	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
commons dbcp2 2.7.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
commons io 2.7	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
commons lang3 3.10	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
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.
failsafe 2.0.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Geronimo 1.3	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.

Keyword	Description
Google Guice 4.2.3	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.
Jakarta Commons Projects	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
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.
Jansi 1.18	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
jcommander 1.71	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
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.
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.
Log4j 2.17.1	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Okio 1.15.0	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Opensaml 3.4.5	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
p6spy 3.8.6	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
Primefaces 7.0	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 7.37.2	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.
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.
Wink 1.1.3	Specific library and version used by the TOE. Version was used to narrow the library search to only relevant records.

The search teams and public sources were expanded from those used in the original evaluation. The most notable change being that the search terms for this maintenance action included all of the third party libraries while those library names were not covered in the original evaluation. The searches did not have a cutoff date. So residual vulnerabilities in the original evaluated product that would have been found with the expanded terms and databases would have shown up in this search. So this analysis also demonstrates that those vulnerabilities were fixed in this version of the 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:

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 v8.2p2 had no impact on the certified TOE.

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

Also, the developer confirmed the changed TOE conforms to NIAP Policy 5, and the existing CAVP certs were found to still be valid.

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