1Password SCIM Bridge Security Assessment

Project No. 378.2207
Report
FINAL

for

AgileBits Inc dba 1Password
4711 Yonge St., 10th Floor
Toronto, ON M2N 6K8
Canada

Document Versions and Changes

Version	Author	Date	Comment
0.1	Johan Rydberg Möller	2022-12-27	Initial draft
0.2	Sascha Schirra	2022-12-28	Technical review
0.3	Florian Grunert	2023-01-03	Additions
0.4	Nico Lindner	2023-01-06	Editorial review
0.5	Johan Rydberg Möller	2023-01-08	Clarifications
0.6	Johan Rydberg Möller	2023-01-09	Additions
0.7	Nico Lindner	2023-01-09	Review
0.8	Nico Lindner	2023-03-13	Incorporating feedback of AgileBits
1.0	Nico Lindner	2023-03-13	Final version

Table of Contents

1 Executive Summary....5
2 Project Background....6
2.1 Team....6
2.2 Analyzed System....7
2.3 Procedures....8
2.3.1 Source Code Review....8

Terms and Definitions

Term	Definition
OWASP	Open Web Application Security Project
SCIM	System for Cross-domain Identity Management
URL	Uniform Resource Locator

1 Executive Summary

Recurity Labs was tasked to perform a security assessment of the Google Workspace integration via SCIM Bridge in 1Password[1].

1Password SCIM Bridge is a well-tested part of the 1Password infrastructure. However, the integration with Google Workspace contains a large amount of new code and functionality, which has not previously been tested, and is not part of the SCIM protocol. In particular, the communication and networking as well as credential handling parts of the service are largely new, and have therefore been put in-scope of this assessment, focusing on credential handling, user and group synchronization and authentication and cryptographic functions. The assessment included both dynamic and automated testing as well as a cursory source code review.

It must be noted that the assessment was time-boxed, so that the review must not be considered exhaustive. However, the areas mentioned above have been tested as far as possible within the allowed time. Based on this and the fact that no findings of any security-relevant observations were discovered during testing, the solution appears to be sound and with a good security posture.

1 https://support.1password.com/scim/

2 Project Background

While the 1Password SCIM Bridge is a well tested part of the 1Password application, the new integration with Google Workspace contains a large amount of new functionality, which should be tested and has therefore been put in-scope of this security assessment.

Unlike other integrations utilizing the SCIM protocol, the new integration with Google Workspace relies on a different communication paradigm, leveraging the Google AdminAPI to register webhooks for directory events, and to poll the Google User Directory. The details regarding the new functionality and the areas of interest for this test were shared in the file `Q4-22_1Password_SCIM_Bridge.pdf`.

Additional details were shared in the following files:

File/Document Name	Received	Content
`[RFD 0030] User Provisioning for Google Workspace.pdf`	2022-12-12	User provisioning for Google Workspace
`[RFD 0034] Group Provisioning for Google Workspace.pdf`	2022-12-12	Group Provisioning for Google Workspace - Adding automated group provisioning support to Google Workspace
`op-main.zip`	2022-12-12	Source code for 1Password SCIM Bridge
`Q4-22_1Password_SCIM_ Bridge.pdf`	2022-12-12	1Password SCIM Bridge - Security Assessment introduction
`scimsession`	2022-12-12	Session information
`URLs.txt`	2022-12-12	URL for 1Password SCIM Bridge and b5 test environment

2.1 Team

The review was performed by Johan Rydberg Möller of Recurity Labs in the time period between December 12th and 16th, 2022. Support was provided by AgileBits whenever requested. Florian Grunert of Recurity Labs served as the responsible project manager.

2.2 Analyzed System

The consultant was given access to a test account, `johan_google@recurity-labs.de`, and the environment located at `pentesttempaccount.b5test.com` as well as the 1Password SCIM Bridge application itself, located at `ptta.op-scim-demo.com`. Temporary accounts were created to test user sync and has since been removed. The integration was performed using Recurity Labs' own Google Workspace account(s).

Furthermore, access to documentation outlining the user and groups provisioning procedures, and test notes describing previous security issues and areas of concern, was provided.

Access to the source code for the 1Password SCIM Bridge application, written primarily in Go, was granted, which appeared as outlined below:

```
github.com/AlDanial/cloc v 1.92  T=12.10 s (394.8 files/s, 125236.9 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Go                            4029         106680         146662         909682
C                                4          15534          74212         150028
JSON                            37              2              0          32542
Markdown                       256           9573              0          19918
Assembly                        50           1704           1334           6519
Bourne Shell                   167           1716           1421           6479
YAML                            72            370            256           4869
TypeScript                      66            568            162           3999
C/C++ Header                     3            349          10919           2340
make                            34            439            169           1485
XML                              2              0              1           1173
Protocol Buffers                12            262            109            853
yacc                             1             41              4            482
Bourne Again Shell               3             46             57            407
reStructuredText                 1            194            442            252
Dockerfile                      22            116             41            218
JSON5                            1              1             15            154
Ruby                             1             23              3             84
JavaScript                       4              2              8             60
Objective-C                      1             13              7             47
Python                           1             20              1             47
TOML                             3             14             25             41
HTML                             1              2              0             18
awk                              2              8              6             18
SVG                              1              0              0             12
PowerShell                       1              2              2              5
CSS                              1              0              0              3
NAnt script                      1              0              0              2
-------------------------------------------------------------------------------
SUM:                          4777         137679         235856        1141737
-------------------------------------------------------------------------------
```

2.3 Procedures

The 1Password SCIM Bridge application, located at `ptta.op-scim-demo.com` has been manually tested for common OWASP Top 10 vulnerabilities as well as for specific scenarios regarding user spoofing, authentication bypass, log file tampering, path traversal, token manipulation and reuse and more.

The 1Password application has been reviewed in a similar manner, focusing on authentication, integration and user provisioning. Both applications have also been tested by attempting to create harmful scenarios from the Google Workspace side, by editing user data and groups, attempting to bypass credential restrictions or access user secrets and vaults, and attempting race conditions during user and group syncs.

Automated testing has also been performed in order to discover instances of request smuggling and cache poisoning.

2.3.1 Source Code Review

Were applicable, a cursory source code inspection has been performed for the provided repository, within the time constraints of the project. The review focused on the identification of general coding mistakes and logic flaws that may be difficult to find using dynamic testing, as well as looking for complex bugs related to the communication, authentication and provisioning parts of the application, such as poor cryptographic implementation, race conditions (within user and group sync), departures from Go security best practices, hidden or unused functionality, etc. The code base has also been reviewed for hardcoded secrets.