Release Notes for OX Dovecot Pro Patch Release v2.3.14.1

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.14.1
Built on Dovecot Community Edition Core v2.3.14
Including Object Storage (obox) and Full Text Search (FTS) Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS 7.9, 8.3
- RHEL 7.4, 8.2
- Debian stretch (9.13), buster (10)
- Ubuntu 18.04 LTS (bionic), 20.04 LTS (focal)

Apache Cassandra Driver: v2.15.3

2. Release Highlights

SECURITY FIXES

This release fixes two security issues. **It is recommended that installations of OX Dovecot Pro that are directly affected by these issues upgrade to this version as soon as possible.** Further details will be made available when the issues are disclosed to the public.

Open-Xchange has no knowledge of these exploits being used as targeted attacks in the wild.

The release notes are CONFIDENTIAL and restricted to OX Dovecot Pro customers only. Public disclosure of the CVE issues will occur on or after 21 June 2021.

OAUTH Escaping

OX Dovecot Pro did not correctly escape `kid` and `azp` fields in JWT tokens. This can be used to supply attacker-controlled keys to validate tokens.

This is problem with fs-posix only. Thus, this is a local vulnerability and requires that the attacker can place files in the local filesystem for the server. *This is not a typical configuration for OX Dovecot Pro installations, which normally do not give users direct access to the mail server filesystems*.

If local validation of JWT is used and the `azp` or `kid` (keyid) fields in JWT tokens contain '`/`' or '`%`' characters, these need to be escaped in the dictionary that stores the local validation keys. Escaping is done by substituting '`/`' with "`%2f`" and '`%`' with "`%25`" respectively. If using dict-fs, and in the unlikely case that either of these fields contains only '`.`' characters, these need to be escaped with "`..`" for every dot.

Workaround:

- Configure a different storage technology, e.g., Redis, to store the keys.

CVE-2021-29157; CVSS Score: 6.7
(CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

Submission STARTTLS Command Injection

Submission service allows on-path attacker to inject commands after STARTTLS issued by client that would get executed after STARTTLS negotiation has taken place. This exploit only affects submission service, *not* LMTP.

Workaround:

- None (outside of disabling submission service)

CVE-2021-33515; CVSS Score: 4.2
(CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N)

Summary of Highlights

- Fix security issues CVE-2021-29157, CVE-2021-33515.

3. Upgrade Information

No Changes

4. Known Issues

- Filter rules will crash if '?' is used. Workaround: quote filter values with wildcards (i.e., use `status="2??"` instead of `status=2??`).
- OX Dovecot Pro might unnecessarily log an error "Failed to add attachment keywords: mail_get_parts() failed: Mail field not cached". There is no user visible impact, but if the log line disrupts operations, it is possible to disable the opportunistic attachment detection by adding the `no-flags-on-fetch` option to `mail_attachment_detection_options`.
- Not all Dovecot 2.2.x logging has been converted to Dovecot 2.3.x events, so newer logging/metrics configuration will not work on these older log entries.

5. Detailed Changes

5.1. OX Dovecot Pro Core

- **SECURITY DOV-4489**: OX Dovecot Pro did not correctly escape `kid` and `azp` fields in JWT tokens. This can be used to supply attacker-controlled keys to validate tokens. (CVE-2021-29157)

- **SECURITY DOV-4586**: On-path attacker could inject plaintext commands before STARTTLS negotiation that would be executed after STARTTLS finished with the client. (CVE-2021-33515)

5.2. Object Storage (obox) Plug-in

No Changes

5.3. Full Text Search (fts) Plug-in

No Changes

5.4. Pigeonhole (sieve) Plug-in

No Changes

5.5. Intercept (intercept) Plug-in

No Changes

6. Tests

The QA team has successfully verified all issue fixes that could be reproduced within a lab environment.

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server setup for system and integration testing.

All changes have been checked for potential side-effects and effect on behavior. Unless explicitly stated within this document, we do not expect any side-effects.

7. Repository Information

For details of how to install and update OX Dovecot Pro, please refer to the instructions at:
https://doc.dovecot.org/installation_guide/dovecot_pro_releases/repository_guide/.