Release Notes for OX Dovecot Pro Patch Release v2.2.36.7

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.2.36.7
Including Object Storage (obox) and Full Text Search (FTS) Plug-ins

Supported OS Distributions:

- CentOS 6.9, 7.8
- Debian wheezy (7.11), jessie (8.11), stretch (9.12)
- RHEL 6.5, 7.0
- Ubuntu 14.04 LTS, 16.04 LTS

2. Release Highlights

SECURITY FIX

This release fixes a security issue. It is urged that all installations of OX Dovecot Pro running v2.2.x upgrade to apply the fix. Further details will be made available when the issues are disclosed to the public.

These vulnerabilities were discovered by a responsible third party. 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 15 July 2020.

Note: this release also fixes two additional authentication related CVE's contained in Dovecot Community Edition Core, CVE-2020-12673 and CVE-2020-12674. Neither of these affect OX Dovecot Pro as the authentication methods affected (NTLM, RPA) are not supported in Pro.

Deeply Nested MIME Structures

Parsing mails with many MIME parts could have resulted in excessive CPU usage or a crash due to running out of stack memory.

This issue is present in Dovecot since it was first released.

Fix: MIME nesting limits have been added.

CVE-2020-12100; CVSS Score: 7.5 (CVSS3.1:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Summary of Highlights

- Fix security issue CVE-2020-12100
- Added auto-truncation of large index cache files instead of requiring admin to manually delete these files.
- Fix metacache cleaning logic

3. Detailed Changes

3.1. Dovecot Pro Core

- **SECURITY DOV-3964:** Parsing mails with a large number of MIME parts could have resulted in excessive CPU usage or a crash due to running out of stack memory.
  - Nested MIME part count is now limited to 100. When the limit is reached, the innermost MIME part's body contains all the rest of the inner bodies until a parent MIME part is reached.
  - Total number of MIME parts is now limited to 10000. When it's reached, no more MIME boundary lines will be recognized, so the rest of the mail belongs to the last added MIME part.

- **ISSUE DOV-3292**: Merging indexes for non-INBOX namespace crashes with: Panic: file mail-namespace.c: line 768 (mail_namespace_find_inbox): assertion failed: (namespaces != NULL)

- **ISSUE DOV-3974**: Writing to >=1 GB dovecot.index.cache files may cause assert-crashes: Panic: file mail-index-util.c: line 37 (mail_index_uint32_to_offset): assertion failed: (offset < 0x40000000)

3.2. Object Storage (obox) Plug-in

- **ISSUE DOV-3812**: Metacache cleaning did not free disk space for users in exactly the correct order. This could have resulted in inefficient metacache behavior or even stop metacache cleaning entirely and cause it to exceed its maximum size.

- **ISSUE DOV-3977**: When there were "temporarily lost" emails, saving a mail could have caused duplicate mail deliveries.
  - This was logged as: Error: Mailbox INBOX: Mail with OID=... was already added by another process to UID=... - leaving it and aborting transaction

3.3. Full Text Search (fts) Plug-in

No Changes

3.4. Pigeonhole (sieve) Plug-in

- **ISSUE DOV-3481**: Users received duplicate mails when a temporary failure occurred at runtime. Temporary runtime failures are not common in normal Pigeonhole execution; only the metadata extension and some proprietary plugins can currently trigger one. Temporary failures in the final action execution (after the script itself is evaluated) do not trigger this problem.

3.5. OX Engage (imap-injection) Plug-in

No Changes

3.6. Chat Over Imap (coi) Plug-in [beta]

No Changes

3.7. Intercept (intercept) Plug-in

No Changes

4. 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.

5. 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/.