Release Notes for OX Dovecot Pro Minor Release v2.3.15

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.15
Built on Dovecot Community Edition Core v2.3.15
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

This is a maintenance release of OX Dovecot Pro v2.3 branch, which contains security fixes, bug fixes, and feature additions.

High Availability Shared Mailboxes

Previously, OX Dovecot Pro only supported mailbox sharing when all users accessed a mailbox on the same server. As of this release, mailbox sharing is now available across a cluster. All users accessing a mailbox will be transparently proxied to a single Dovecot backend that handles all accesses to the mailbox.

See https://doc.dovecot.org/configuration_manual/shared_mailboxes/cluster_setup for further information.

Configuration Support for TLSv1.3 Settings

The new version provides configuration support for TLSv1.3 settings (see `ssl_cipher_suites` and `ssl_min_protocol` settings).

Improved Obox Retry Delays

Previously, temporary errors when accessing storage with obox would have immediately retried multiple times before returning an error. Now, these retry delay grows between attempts to allow the storage to recover from temporary errors.

The new retry times are 50ms -> 500ms -> 5s -> 10s. Retries happen for all 5xx errors as well as for 423 (locked) with sproxyd and 409 (conflict) with CDMI.

Improved Process Launching Performance

For heavily loaded servers, new processes were not being launched quickly enough in certain situations, causing various problems. Process launching performance has been improved as of this version.

SECURITY FIX

This release fixes three 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 JWT 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.

Example:

Note: this issue is also fixed in OX Dovecot Pro v2.3.14.1.

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)

Sieve Denial of Service

The Sieve interpreter is not protected against abusive scripts that claim excessive resource usage.

Workarounds:

- Disable Sieve "regex" extension
- Limit CPU usage of Sieve scripts

CVE-2020-28200; CVSS Score: 4.3
(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

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.

Note: this issue is also fixed in OX Dovecot Pro v2.3.14.1.

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

- Add support for high availability mailbox sharing.
- Add configuration support for TLSv1.3 settings.
- Improve retry delays when obox encounters temporary storage errors.
- Improve process launching performance when master service rapidly forks many processes.
- Fix security issues: CVE-2020-28200, CVE-2021-29157, CVE-2021-33515
- Removed support for Lua 5.2.

3. Upgrade Information

The default value for `ssl_min_protocol` changed from `TLSv1` to `TLSv1.2`. TLS 1.0 and TLS 1.1 were deprecated in 2020. (See RFC 8996: https://datatracker.ietf.org/doc/html/rfc8996). OX Dovecot Pro aims to be secure by default, so the minimum allowable TLS version was changed to match best current practices for security. Administrators willing to allow mail clients to use these insecure, deprecated TLS methods to connect can explicitly set the value of `ssl_min_protocol` in the Dovecot configuration file. See https://doc.dovecot.org/settings/core/#ssl-min-protocol for details on that setting.

Certain advanced settings are now hidden by default when using doveadm/doveconf.

Support for Lua 5.2 has been removed. Reducing the amount of version specific code allows easier extension of Dovecot Lua APIs. Some future features might support Lua 5.3+ only. Depending on Linux distribution, Dovecot packages now depend on either Lua 5.1 or Lua 5.3. If custom Lua scripts require module dependencies that are not available in your OS distribution, it is recommended to use the LuaRocks module package manager.

IMAP PREVIEW now supports the finalized RFC 8970 standard. The previous Dovecot-specific IMAP commands to retrieve preview information have been deprecated. See: https://doc.dovecot.org/admin_manual/imap_preview/

Change the language name for Japanese in kuromoji plugin from `jp` to `ja`. This should be changed in the configuration; using the old value will give a warning.

TLS v1.3 settings are now supported in Dovecot configuration. See:

- https://doc.dovecot.org/settings/core/#ssl-cipher-suites
- https://doc.dovecot.org/settings/core/#setting-ssl-min-protocol

Added settings:

- `acl_ignore_namespace` (https://doc.dovecot.org/settings/plugin/aclPlugins/index.html#acl-ignore-namespace)
- obox plugin: Added `avoid_423` parameter for sproxyd. See: https://doc.dovecot.org/configuration_manual/mail_location/obox/scality_sproxyd/

Changed settings:

- Compression level configuration now allows per-algorithm values instead of being hard-coded to gzip defaults (1-9, default 6). See, e.g., https://doc.dovecot.org/configuration_manual/zlib_plugin/

Added events (see https://doc.dovecot.org/admin_manual/list_of_events/):

- `fts_dovecot_too_many_triplets`
- `indexer_worker_indexing_finished`
- `mail_cache_lookup_finished`
- `mail_expunged`
- `mail_expunge_requested`
- `mail_opened`

Changed logging:

- metacache-worker no longer logs an Info log line when it has cleaned a user from metacache. This can still be done by exporting the `metacache_user_clean_finished` event.
- Disconnection log messages are now more standardized across services. They also always now start with "Disconnected" prefix.

4. Known Issues

- Filter rules will crash if '?' is used. This will be fixed in the next version of Dovecot. 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". This will be fixed in the next version of Dovecot. 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-4583**: On-path attacker could inject plaintext commands before STARTTLS negotiation that would be executed after STARTTLS finished with the client. (CVE-2021-33515)

- **IMPROVEMENT DOV-4266**: Support official RFC 8970 preview/snippet syntax. Old methods of retrieving preview information via IMAP commands ("SNIPPET and PREVIEW with explicit algorithm selection") have been deprecated.

- **IMPROVEMENT DOV-4306**: New SSL/TLS settings.
  - Add TLSv1.3 support to `ssl_min_protocol`.
  - Allow configuring `ssl_cipher_suites` for TLSv1.3+.

- **IMPROVEMENT DOV-4317**: Make the health-check.sh example script POSIX shell compatible.

- **IMPROVEMENT DOV-4323**: Add `acl_ignore_namespace` setting which allows to entirely ignore ACLs for the listed namespaces. See: https://doc.dovecot.org/settings/plugin/aclPlugins/index.html#acl-ignore-namespace

- **IMPROVEMENT DOV-4350**: Convert indexer-worker "Indexed" info logs to an event named "`indexer_worker_indexing_finished`", emitted on DEBUG level, with these extra fields:
  - `message_count`: Number of messages indexed
  - `first_uid`: First uid of the message indexed
  - `last_uid`: Last uid of the message indexed
  - `user_cpu_usecs`: Total user mode cpu time spent on indexing

- **IMPROVEMENT DOV-4353**: Support compression levels that the algorithm supports. Before, we would allow hardcoded value between 1 to 9 and would default to 6. Now we allow using per-algorithm value range and default to whatever default the algorithm specifies.

- **IMPROVEMENT DOV-4442**: Support INDEXPVT for imapc storage to enable private message flags for cluster wide shared mailboxes (NFS only).

- **IMPROVEMENT DOV-4454**: New mail events added:
  - `mail_opened`
  - `mail_expunge_requested`
  - `mail_expunged`
  - `mail_cache_lookup_finished`

- **CHANGE DOV-3982**: Some settings are now marked as "hidden". It is discouraged to change these settings. They will no longer be visible in doveconf output, except if they have been changed or if “doveconf -s” parameter is used.
  - Most mail_index_* and mail_cache_* settings are now hidden.

- **CHANGE DOV-4376**: Disconnection log messages are now more standardized across services. They also always now start with "Disconnected" prefix.

- **CHANGE DOV-4433**: Removed support for Lua 5.2. Use version 5.1 or 5.3 instead.

- **ISSUE DOV-1679**: IMAP BINARY FETCH crashes at least on empty base64 body.
  - *Fixes*: Panic: file index-mail-binary.c: line 358 (blocks_count_lines): assertion failed: (block_count == 0 || block_idx+1 == block_count).

- **ISSUE DOV-3979**: Index rebuilding (e.g., via “doveadm force-resync”) didn't preserve the "hdr-pop3-uidl" header. Because of this, the next pop3 session could have accessed all the emails' metadata to read their POP3 UIDL (opening dbox files, HEADing obox objects).

- **ISSUE DOV-4154**: Systemd service: Dovecot announces readiness for accepting connections earlier than it should. The following environment variables are now imported automatically and can be omitted from `import_environment` setting: `NOTIFY_SOCKET LISTEN_FDS LISTEN_PID`.

- **ISSUE DOV-4250**: Dsync issues with shared mailboxes.
  - Shared namespaces were not synced with "-n" flag.
  - Syncing shared INBOX failed if `mail_attribute_dict` is not set.
    - If a user has a shared mailbox that is another user's INBOX, dsync failed to export the mailbox if mail attributes are disabled.

    - Shared INBOX not synced when "`mail_shared_explicit_inbox`" is disabled.
        - If a user has a shared mailbox which is another user's INBOX, dsync did not include the mailbox in syncing unless explicit naming is enabled with "`mail_shared_explicit_inbox`" set to "`yes`".

- **ISSUE DOV-4319**: Dovecot would incorrectly fail with haproxy 2.0.14 service checks.

- **ISSUE DOV-4335**: Using IMAP COMPRESS extension can cause IMAP connection to hang when IMAP commands are >8 kB long.

- **ISSUE DOV-4336**: Commands pipelined together with and just after the authenticate command cause these commands to be executed twice. This applies to all protocols that involve user login, which currently comprises of imap, pop3, submission and managesieve.

- **ISSUE DOV-4361**: If IMAP client using the NOTIFY command disconnects while Dovecot is sending FETCH notifications to the client, Dovecot may crash.
    - *Fixes*: Panic: Trying to close mailbox INBOX with open transactions.

- **ISSUE DOV-4362**: The LMTP proxy crashes with a panic when the remote server replies with an error while the mail is still being forwarded through a DATA/BDAT command.

- **ISSUE DOV-4365**: Username may have been missing from lmtp log line prefixes when it was performing autoexpunging.

- **ISSUE DOV-4371**: Many events were missing the parent event hierarchy. This affects too many events to list individually, but most importantly dict-related events, dns-lookup-related events, and some http-related events.

- **ISSUE DOV-4384**: Using both Solr FTS and Tika may have caused HTTP requests to assert-crash: Panic: file http-client-request.c: line 1232 (http_client_request_send_more): assertion failed: (req->payload_input != NULL)
    - v2.3.13 tried this fix this already, but it did not fully work.

- **ISSUE DOV-4387**: imapc may go to infinite busy-loop if remote server sends BYE but does not immediately disconnect.

- **ISSUE DOV-4399**: v2.3.11 regression: Indexing messages with fts-tika may have resulted in panic.
    - *Fixes*: file message-parser.c: line 802 (message_parser_deinit_from_parts): assertion failed: (ctx->nested_parts_count == 0 || i_stream_have_bytes_left(ctx->input))

- **ISSUE DOV-4402**: `service { process_min_avail }` was launching processes too slowly when master was forking a lot of processes.

- **ISSUE DOV-4406**: imap/pop3/managesieve/submission-login processes are supposed to disconnect the oldest non-logged in connection when `process_limit` was reached. This did not actually happen with the default "high-security mode" (`service_count=1`) where each connection is handled by a separate process.

- **ISSUE DOV-4411**: Checking hostnames against an SSL certificate must be case-insensitive.

- **ISSUE DOV-4413**: Userdb iteration with passwd driver does not always return all users with some nss drivers.

- **ISSUE DOV-4417**: fts-tika treated 5xx errors returned by Tika server as indexing failures. However, Tika can return 5xx for some attachments every time. So, the 5xx error should be retried once, but treated as success if it happens on the retry as well. v2.3 regression.

- **ISSUE DOV-4436**: When login process reaches client/process limits, oldest client connections are disconnected. If one of these was still doing anvil lookup, this caused a crash. This could happen only if the login process limits were very low or if the server was overloaded.
    - *Fixes*: Panic: file client-common.c: line 299 (client_destroy): assertion failed: (!client->authenticating)

- **ISSUE DOV-4437**: Corrupted cache record size in dovecot.index.cache file could have caused a crash (segfault) when accessing it.

- **ISSUE DOV-4469**: LMTP connection crashes if connection gets disconnected due to multiple bad commands and the last bad command is BDAT.

- **ISSUE DOV-4477**: When using the listescape plugin and a shared namespace the plugin did not work properly anymore resulting in errors like: "Invalid mailbox name: Name must not have '/' character."

- **ISSUE DOV-4508**: Corrupted mime.parts in dovecot.index.cache may have resulted in panic.
    - *Fixes*: Panic: file imap-bodystructure.c: line 206 (part_write_body): assertion failed: (text == ((part->flags & MESSAGE_PART_FLAG_TEXT) != 0))
    - This panic is v2.3.13 regression. Earlier versions just ignored the corruption.

- **ISSUE DOV-4510**: The Dovecot-specific LMTP parameter XRCPTFORWARD is blindly forwarded by LMTP proxy without checking that the backend has support. This causes a command parameter error from the backend if it is running an older Dovecot release. This can only occur in more complex setups where the message is proxied twice; when the proxy generates the XRCPTFORWARD parameter itself the problem does not occur, so this only happens when it is forwarded.

- **ISSUE DOV-4516**: Duplicate folder names in dovecot.list.index were detected only for root folders, not for child folders. This prevented Dovecot

from fixing the duplicates automatically. It should not be possible for users to cause this situation normally.

- **ISSUE DOV-4532**: SETMETADATA could not be used to unset metadata values. Instead, NIL was handled as a "NIL" string. v2.3.14 regression.

- **ISSUE DOV-4546**: In huge folders it was possible to have multiple long-running IMAP MOVE commands processing the same mails. This could have caused duplicate mails in the destination folder. Note that some duplication can still happen even with this fix, but the extra MOVEs are expected to stop much earlier.

5.2. Object Storage (obox) Plug-in

- **IMPROVEMENT DOV-4331**: Grow retry intervals more. Previously the initial retry time has been doubled per attempt, now the wait time becomes multiplied by ten to give the resource more time to recover. The new retry times are 50ms -> 500ms -> 5s -> 10s. The maximum wait time before retry is limited to 10 seconds. Retries happen for 5xx errors as well as for 423(locked) with sproxyd and 409(conflict) with CDMI.

- **IMPROVEMENT DOV-4354**: fs-sproxyd: Added `avoid_423=<time>` parameter. This delays DELETE requests if the same object ID has been GET/HEAD/PUT by the same process within <time>. This is intended to reduce "423 Locked" sent by Scality. Enable this with, e.g., `obox_fs = ...&class=2&avoid_423=500ms`.

- **CHANGE DOV-4369**: metacache-worker no longer logs an Info log line when it has cleaned a user from metacache. This can still be done by exporting the `metacache_user_clean_finished` event.

- **ISSUE DOV-4405**: If the `delete-dangling-links` option was set, there was no `fs_dictmap_object_lost` event emitted. Now the event is emitted, and it has an additional "`deleted`" field. A warning is logged as well if the deletion was successful. For more information on the event refer to https://doc.dovecot.org/admin_manual/list_of_events/#fs-dictmap-object-lost.

- **ISSUE DOV-4509**: If metacache has a TX-ROLLBACK command pending while trying to deinitialize worker connections it could have crashed. This could have only happened when stopping Dovecot.

5.3. Full Text Search (fts) Plug-in

- **IMPROVEMENT DOV-4279**: Added `fts_dovecot_max_triplets` setting. If the number of FTS triplets is more than this, the indexing or search will fail immediately. This setting can be used to avoid excessive slowness due to earlier bugs that caused the number of triplets to be huge.
    - When this happens, an error is logged and `fts_dovecot_too_many_triplets` event is sent.

- **IMPROVEMENT DOV-4303**: Added `file_type=fts` field to FTS fs access events. Added `fts` category to all FTS events.

- **ISSUE DOV-3823**: Change the language name for Japanese in kuromoji plugin from jp to ja.

- **ISSUE DOV-4272**: Using NOT HEADER search for any header other than From, To, Cc, Bcc and Subject did not return correct results.

5.4. Pigeonhole (sieve) Plug-in

- **SECURITY DOV-4159**: Sieve interpreter is not protected against abusive scripts that claim excessive resource usage. Fixed by limiting the user CPU time per single script execution and cumulatively over several script runs within a configurable timeout period. Sufficiently large CPU time usage is summed in the Sieve script binary and execution is blocked when the sum exceeds the limit within that time. The block is lifted when the script is updated after the resource usage times out. (CVE-2020-28200)

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/.