Release Notes for Dovecot Pro Minor release 2.2.34

1. Shipped Products and Versions

Dovecot Pro 2.2.34
Including Object Storage Plug-in, Full Text Search Plug-in, Full Text Search Kuromoji Plug-in, Pigeonhole Sieve Plug-in and Dovemon

1.1. Dovecot Pro Core

- **BUG DOV-1933: SECURITY BUG** (CVE-2017-15130): TLS SNI config lookups are inefficient and can be used for DoS. If Dovecot has been configured with local_name {...} or local {...} configuration blocks, SNI lookups can be used to fill up memory with useless config by using random servernames. This eventually reaches the imap-login/pop3-login process's VSZ limit and restarts the process.

- **BUG DOV-1702: SECURITY BUG** (CVE-2017-14461): Parsing invalid email addresses may cause a crash or leak memory contents to attacker. For example, these memory contents might contain parts of an email from another user if the same imap process is reused for multiple users. First discovered by Aleksandar Nikolic of Cisco Talos. Independently also discovered by "flxflndy" via HackerOne.
    - **FIX:** lib-mail: Fix out-of-bounds read when parsing an invalid email address
    - **FIX:** lib-mail: Make sure parsers don't accidentally go much beyond end pointer

- **BUG DOV-1695: SEURITY BUG** (CVE-2017-15132): Aborted SASL authentication leaks memory in login process
    - **FIX:** lib-auth: Fix memory leak in auth_client_request_abort()

- **BUG DOV-1471: SECURITY BUG**: Using PR_SET_DUMPABLE can bypass chroot/group restrictions
    - **FIX:** lib: Call prctl(PR_SET_DUMPABLE) only when PR_SET_DUMPABLE env variable is set
    - Dovecot enabled PR_SET_DUMPABLE for most of the processes to allow them to create core dumps. However, processes that have this enabled also allow them to ptrace() each others, as long as they're using the same UNIX UID. This can be used by attackers to bypass other security features, such as processes using different GIDs or chrooting.
        - For example a local user could ptrace() their own imap process, which has mail_access_groups set to a GID that the user normally wouldn't have access to.
    - In Linux core dumps can be safely enabled nowadays by setting sysctl fs.suid_dumpable=2

    - If the old behaviour is wanted, it can still be enabled by setting: import_environment=$import_environment PR_SET_DUMPABLE=1
    - Found by cPanel Security Team

- **NEW FEATURE DOV-1221:** Attachment indicator
    - Mark email attachment presence using $HasAttachment / $HasNoAttachment keywords. By default, all MIME parts with Content-Disposition=attachment, or inlines with filename parameter are consired attachments. A new mail_attachment_detection_options setting controls how and when they're set:
        - add-flags-on-save — Add the keywords when saving mail (required to enable this)
        - content-type=type or !type — Include/exclude content type. Excluding will never consider the matched MIME part as attachment. Including will only negate an exclusion (e.g. content-type=!foo/* content-type=foo/bar).
        - exclude-inlined — Exclude any Content-Disposition=inline MIME part.

- **NEW FEATURE DOV-1285:** Fetch body snippets over IMAP
    - imap: Add support for fetching body snippets using FETCH (SNIPPET) or (SNIPPET (LAZY=FUZZY)).

- **IMPROVEMENT DOV-1423:** fs-compress: Automatically detect whether input is compressed or not
    - Prefix the compression algorithm with "maybe-" to enable the detection, for example: "compress:maybe-gz:6:..."
    - Use compress level 0 to disable writing compressed files, but still be able to read compressed files.

- **IMPROVEMENT DOV-1434:** lib-index: Make hardcoded index behavioral parameters configurable
    - Added settings to change dovecot.index* files' optimization behavior. It's not recommended to change these settings without fully understanding the consequences.
      See https://wiki2.dovecot.org/IndexFiles#Settings

- **IMPROVEMENT DOV-1435:** auth: Move password hash verification to auth-workers
    - Auth cache can now utilize auth workers to do password hash verification.

- **IMPROVEMENT DOV-1718:** Include hostname in doveconf output.

- **IMPROVEMENT DOV-1438:** Support Japanese special charset conversions
    - Added charset_alias plugin. It allows treating the specified source charset as a different charset when decoding to UTF-8. For instance, when decoding from shift_jis to UTF-8, using cp932 (or sjis-win) instead of shift_jis may be preferable to handle Microsoft extended chars properly.
      See https://wiki2.dovecot.org/Plugins/CharsetAlias

- **IMPROVEMENT DOV-1519:** imapc: Expunged mail returned as empty
    - imapc: Add imapc_features=fetch-empty-is-expunged. When FETCH returns an empty mail, the mail is assumed to be expunged.

- **IMPROVEMENT DOV-1643:** *_logout_format does not support all variables, like userdb variables or %rip
    - imap_logout_format and pop3_logout_format settings now support all of the generic variables (e.g. %{rip}, %{session}, etc.)

- **IMPROVEMENT DOV-1921:** imapc: Don't disconnect on broken untagged IMAP replies. Try to skip over the line and continue. This may allow imapc to work around broken input sent by some IMAP servers.

- **BUG/IMPROVEMENT DOV-1771:** dovecot uses master username in before authentication policy lookup
    - BUG: With master user logins, the master username is used in before authentication policy lookups
        - FIX: auth: Use login username in auth policy requests
    - IMPROVEMENT: Add auth_policy_check_before_auth, auth_policy_check_after_auth, and auth_policy_report_after_auth tunables to control which auth policy requests are enabled

- **BUG 51975/DOV-757:** The doveadm HTTP server crashes when trying to disconnect client at deinit.
    - **FIX:** Restructured client connection deinit code so that connection is destroyed only once.

- **BUG 55178/DOV-929:** SEARCH MIME may crash with: Panic: file index-mail-headers.c: line 296 (index_mail_parse_header): assertion failed: (part != NULL)
    - **FIX:** lib-storage: Fix assert-crash when searching header and MIMEPART

- **BUG 54383/DOV-937:** FTS reindexes all mails unnecessarily after loss of dovecot.index.cache file
    - **FIX:** fts: Don't reindex FTS mails if .cache file is deleted
    - Previously dovecot.index.cache was also repopulated at the same time with the fields from mail_always_cache_fields. This is no longer done either.

- **BUG DOV-1204:** imapc: Reconnection may cause crashes and other errors.
    - Panic: file imapc-sync.c: line 373 (imapc_initial_sync_check): assertion failed: (mail_index_is_expunged(view, lseq) || seq_range_exists(&ctx->mbox->delayed_expunged_uids, luid))
    - Panic: Leaked view for index (in-memory index): Opened in imapc-mailbox.c:47
    - **FIX:** Mailbox state should be fetched immediately after a folder is SELECTed. This should happen before any other commands are re-sent that were waiting for an answer before reconnection.

- **BUG DOV-1237:** lock_method=dotlock caused crashes with autoexpunging was enabled or when folder vsize was attempted to be looked up.
    - **FIX:** lib-storage: mail_storage_lock_create() - add support for dotlocks
    - **FIX:** lib-index: Fix assert-crash with lock_method=dotlock

- **BUG DOV-1372:** fs-dictmap: Detect and fix future Cassandra timestamps
    - **FIX:** fs-dictmap now logs a warning if it finds a timestamp from Cassandra that is in the future.

- **BUG DOV-1548:** doveadm log reopen stopped working in v2.2.33.
    - **FIX:** log: Fix log reopening on SIGUSR1

- **BUG DOV-1550:** v2.2.33 failed when trying to access doveadm UNIX socket that didn't require authentication: "Error: doveadm server sent invalid handshake: ..."
    - **FIX:** doveadm: client - Fix connecting to UNIX sockets that don't need authentication
    - **FIX:** doveadm-server: Fix protocol handshake order

- **BUG DOV-1554:** doveadm-server: Auth "user" lookup may have returned invalid JSON output.
    - **FIX:** doveadm-auth-server: Send comma only if we are sending field too

- **BUG DOV-1576:** fs-crypt silently ignored public/private keys specified in configuration (mail_crypt_global_public/private_key) and just emitted plaintext output.
    - **FIX:** mail-crypt: Do not free global keys if no error has occurred

- **BUG DOV-1608:** mdbox rebuild repeatedly fails with: Error: mdbox map .../dovecot.map.index corrupted: missing map extension
    - **FIX:** mdbox: Fix rebuilding when dovecot.map.index is missing map/ref extension

- **BUG DOV-1626:** doveadm-server: Since v2.2.33 logging may have caused I/O leak and Panic: file ioloop.c: line 127 (io_remove_full): assertion failed: (io->callback != NULL)
    - **FIX:** doveadm-server: Switch to TCP connection's ioloop while sending logs to remote

- **BUG DOV-1641:** Nested %if variables didn't work
    - **FIX:** Support nested variables when determining variable length

- **BUG 56383/DOV-1657:** Since v2.2.33, Cassandra driver leaks memory with Cassandra protocol version 3 (Cassandra v2.1)
    - **FIX:** driver-cassandra: Free statement pool on update

- **BUG DOV-1699:** SSL connections may have been hanging with imapc or doveadm client .
    - **FIX:** lib-imap-client: Fix IO after enabling SSL
    - **FIX:** doveadm: client: Set IO only after enabling SSL

- **BUG DOV-1739:** IMAP capabilities haven't automatically contained SPECIAL-USE since v2.2.30.
    - **FIX:** imap: Iterate over ns settings when deciding to add SPECIAL-USE capability

- **BUG DOV-1740:** IMAP hasn't sent untagged OK/NO storage notifications since v2.2.30.
    - For example: "* OK Stale mailbox lock file detected, will override in 15 seconds"
    - **FIX:** imap: Don't set storage callbacks before namespaces are created

- **BUG DOV-1770:** HTTP requests may sometimes crash with: Panic: file http-client-queue.c: line 737 (http_client_queue_request_timeout): assertion failed: (count > 0)
    - **FIX:** lib: time-util: Fix timeval_cmp_margin() to correctly handle a margin crossing the second boundary.

- **BUG DOV-1796:** mail_always/never_cache_fields changes weren't applied for existing dovecot.index.cache files
    - **FIX:** lib-index: Fix adding forced cache decisions to existing cache files
        - If a field already existed in the cache file, the cache decision from the file was always used. This caused force-decisions to be ignored.
    - **FIX:** lib-index: Fix removal of forced cache decisions from existing cache files
        - The forced-flags are written to the cache file when the file is created. They were also read back, and the force-flag was preserved even when the configuration was removed.
    - **FIX:** lib-index: Write forced cache decision changes immediately to cache file
        - When mail_always/never_cache_fields doesn't match the current caching decisions in the cache file, write the updated decisions to the file.

- **BUG DOV-1805:** program-client sometimes truncated output. This was visible with e.g. Sieve extprograms plugin sometimes truncated output from external programs. This applies to the "vnd.dovecot.filter" and "vnd.dovecot.execute" Sieve extensions.

Applies to both forked programs and programs invoked through the script socket service.
    - **FIX:** Fix bugs in program-client I/O stream handling.

- **BUG DOV-1831:** doveadm-proxy: Debug logging with SSL causes memory corruption
    - **FIX:** lib-ssl-iostream: openssl: Make verbose logging robust against i_debug() writing to stream itself.

- **BUG DOV-1832:** fts: Searching doesn't always work correctly for address headers
    - Address headers were indexed using "data" language, so they also need to be searched using the "data" language.
    - **FIX:** fts: Fix searching SEARCH_HEADER_ADDRESS/COMPRESS_LWSP
    - **FIX:** fts: Fix searching headers with TEXT/BODY

- **BUG DOV-1834:** fs-posix: Directory iteration is broken on NFS with nordirplus mount option
    - **FIX:** fs-posix: Fix iterating directories when readdir() returns DT_UNKNOWN

- **BUG DOV-1835:** replication: dsync sends unnecessary replication notification for changes it does internally.
    - **FIX:** replication: Don't send notification for changes done by dsync transactions
    - **NOTE:** Folder creates, renames, deletes and subscribes still trigger unnecessary replication notifications, but these should be rather rare.

- **BUG DOV-1843:** Since v2.2.33, Cassandra queries didn't set timestamps with with Cassandra protocol version 3 (Cassandra v2.1)
    - **FIX:** cassandra: Fix setting timestamp for transaction queries with v3 protocol

- **BUG DOV-1881:** dsync overrides BROKENCHAR, which prevents migrating invalid mUTF-7 mailbox names.
    - **FIX:** doveadm sync/backup: Don't override BROKENCHAR if it's already set

1.2. Object Storage Plug-in

- **IMPROVEMENT DOV-1634:** metacache: Stop letting in new users when metacache disk space is full
    - Because the metacache disk space stays only approximately at metacache_max_space, this triggers only once the disk space is above metacache_max_space + metacache_max_grace. The default for grace is 1 GB, but that may be too small for some installations.
    - The logins are attempted a few times before they fail with: Metacache is out of disk space, not letting in any more users (... bytes used)

- **IMPROVEMENT DOV-1637:** obox: List index rebuild adds folder names as recovered-lost-folder-* instead of their original names
    - The renaming to original folder name is done after the folder is opened again, but there's no reason why it couldn't be done automatically immediately.

- **IMPROVEMENT DOV-1871:** obox: If mailbox list index is empty on login, try to rebuild the list

- **BUG DOV-1473:** metacache-worker may cause HTTP timeouts when absolut_timeout_msecs is configured and a lot of folders are being uploaded.

    - **FIX:** Add a new metacache_max_parallel_requests setting to throttle the parallel requests. The default is 10.
- **BUG DOV-1583:** Dovecot might choose wrong object-store endpoint in swift if region is used.
    - **FIX:** Consider region and interface together when choosing object-store endpoint

- **BUG DOV-1637:** obox: List index rebuild adds folder names as recovered-lost-folder-* instead of their original names.
    - **FIX:** obox: Make sure recovered-lost-folder gets renamed to its original name when rebuilding.

- **BUG DOV-1742:** fs-s3: Failed multi-request iteration accesses freed memory
    - **FIX:** fs-s3: Make sure iteration doesn't double-free XML parser

1.3. Full Text Search Plug-in

- **BUG DOV-1536:** fts_dovecot was logging debug lines that couldn't be disabled: "Debug: FTS: bubble merge"
    - **FIX:** lib-fts-index: Make debug-logging bubble merges optional.

- **BUG 56066/DOV-1536:** fs-fts-cache: Stale cache.log may cause errors: fts_dovecot: Index keeps changing under us too rapidly
    - **FIX:** plugin: Refresh fs-fts-cache if FTS_INDEX_READ_ERROR_RETRY is returned

1.4. Full Text Search Kuromoji Plug-in

- **IMPROVEMENT DOV-1828:** Kuromoji library was updated
    - Fixed emoji segmentation issues
    - Added input chunking to reduce overall memory usage

1.5. Pigeonhole Sieve Plug-in

- **BUG DOV-1606:** Sieve handling could have assert-crashed with specific path lengths with: Panic: file realpath.c: line 86 (path_normalize): assertion failed: (npath_pos + 1 < npath + asize)
    - **FIX:** lib-sieve: util: realpath: Allocate more space earlier

- **BUG DOV-1735:** Large output from Sieve exprograms "execute" command crashed LMTP.
    - **FIX:** Resolved buffering issue in code that handles output from external program.

1.6. Dovemon

- **BUG DOV-1673:** POP3 SASL authentication fails with long usernames
    - **FIX:** dovemon.py: use base64.b64encode when authenticating with SASL

- **BUG DOV-1517:** vhost count for each monitored backend is fetched and incorrectly not converted from string to int. This breaks later some comparsions and HOST-UP is issued to backends with vhost=0

    - **FIX:** Convert vhost count to integer

- **BUG DOV-1542:** dovemon init script doesn't work in Debian
    - **FIX:** dovemon-initscript.debian: fix path to dovemon.py

- **BUG DOV-1829:** Default values for configuration options are not used when they were not set in config file.
    - **FIX:** Use default values when not set in config file.

2. Tests

The Dovecot QA team has successfully verified all bug 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.