DOVECOT

Release Notes for Dovecot Pro Patch Release v2.2.36.1

Table of Contents

1. Shipped Products and Versions

Dovecot Pro v2.2.36.1
Including Object Storage, Full Text Search, and Pigeonhole Sieve Plug-ins

Supported OS Distributions:

- CentOS 6.99, 7.6
- Debian jessie (8.11), stretch (9.7)
- RHEL 6.5, 7.0
- Ubuntu 14.04 LTS, 16.04 LTS

2. Security Advisory

This release fixes a vulnerability in Dovecot related to SSL client certificate authentication.

Normally, Dovecot is configured to authenticate imap/pop3/managesieve/submission clients using a username/password combination. Some installations have also required clients to present a trusted SSL certificate on top of that. It is also possible to configure Dovecot to take the username from the certificate instead of from the user provided authentication. It is also possible to require no password, instead trusting the SSL certificate as sole proof for authentication.

If the provided trusted SSL certificate is missing the username field, Dovecot should reject authentication. However, vulnerable Dovecot versions will take the username from the user provided authentication fields (e.g. username from the LOGIN command). If there is no additional password verification required, this allows the attacker to login as anyone.

This affects only installations using:

```
auth_ssl_require_client_cert = yes
auth_ssl_username_from_cert = yes
```

An attacker must also have access to a valid trusted certificate without the `ssl_cert_username_field` in it. The default is commonName, which exists in most certificates. This could happen for example if `ssl_cert_username_field` is a field that normally doesn't exist, and attacker has access to a web server's certificate (and key) which is signed with the same CA.

Additionally, `ssl_cert_username_field` setting was ignored with external SMTP AUTH, because none of the MTAs (Postfix, Exim) currently send the ssl_cert_username_field. This may have allowed users with trusted certificate to specify any username in the authentication. Note: this vulnerability does not apply to Dovecot Submission service.

CVE-2019-3814; CVSS Score: 8.2 (AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N)

3. Release Highlights

- CVE-2019-3814 fix
- Allow X-Dovecot-Reason to be added to all requests for S3 and CDMI obox installations

- For obox, fix some POP3 changes incorrectly being marked as important resulting in unnecessary storage bundle uploads

4. Upgrade Instructions

- To enable sending X-Dovecot-Reason header for S3 and CDMI obox drivers, set `reason_header_max_length` to a non-zero value [DOV-2927]. It is recommended to set this value to at least “200”. Example:

```
plugin {
  obox_fs = s3:https://example.com/?reason_header_max_length=200
}
```

- For imapsieve, add new `imapsieve_expunge_discarded` setting which causes messages discarded by a script to be expunged immediately, rather than only being marked as "\Deleted" (which is still the default behavior). Example:

```
plugin {
  imapsieve_expunge_discarded = yes
}
```

5. Detailed Changes

5.1. Dovecot Pro Core

- **SECURITY DOV-2913 [CVE-2019-3814]:** If imap/pop3/managesieve/submission client has trusted certificate with missing username field (ssl_cert_username_field), under some configurations Dovecot mistakenly trusts the username provided via authentication instead of failing
  - ssl_cert_username_field setting was ignored with external SMTP AUTH, because none of the MTAs (Postfix, Exim) currently send the cert_username field. This may have allowed users with trusted certificate to specify any username in the authentication.
  - Note that after this fix all such SMTP authentications will fail instead. It may be necessary to configure separate authentication inside protocol smtp { ... } that won't rely on the ssl_cert_username_field.
  - This bug didn't affect Dovecot's Submission service.

- **ISSUE DOV-2472:** Snippet generation crashed with invalid “Content-Type: multipart”

- **ISSUE DOV-2473:** Reading 0-sized file with maybe-gz (e.g. fts_dovecot_fs=compress:maybe-gz) crashes with: Panic: file istream.c: line 187 (i_stream_read): assertion failed: (stream->eof)

- **ISSUE DOV-2474:** lda/lmtp may have assert-crashed with some Sieve scripts when mail_attachment_detection_options=add-flags-on-save: Panic: file imap-bodystructure.c: line 116 (part_write_body_multipart): assertion failed: (part->data != NULL)

- **ISSUE DOV-2745:** director: Kicking a user crashes if login process is very slow: Panic: file director.c: line 1025 (director_kill_user_callback): assertion failed: (ctx->dir->users_kicking_count > 0)

- **ISSUE DOV-2747:** pop3: With pop3_no_flag_updates=no: If a message is DELEted and also RETRed, it gets expunged at client disconnection even though QUIT hasn't been sent

- **ISSUE DOV-2910:** If folder is missing from dovecot.index.list, force-resync cannot be used to restore it.

- **ISSUE DOV-2921:** Incorrect path for dovemon.py in debian unit file

5.2. Object Storage Plug-in

- **IMPROVEMENT DOV-2927:** Send X-Dovecot-Reason header to fs-s3 and fs-scality.

- **ISSUE DOV-2437:** "doveadm metacache flushall" with -i parameter didn't work correctly when the system had a lot of users with unimportant changes. It was repeatedly looping over the same users with unimportant changes and counting them as flush attempts. This resulted in the command taking a long time and finally failing with: Error: Users keep changing, ... pending changes (... upload attempts, waiting for ... uploads and ... cleans)

- **ISSUE DOV-2849:** fs-azure: Fix copying mails. The copy PUT requests were failing with: 403 Server failed to authenticate the request. Make sure the value of Authorization header is formed correctly including the signature.

- **ISSUE DOV-2895:** When mailbox size was >= obox_max_rescan_mail_count any changes were marked as being important, causing unnecessary index bundle uploads.
    - FIX: POP3: Don't mark changes as important unnecessarily

5.3. Pigeonhole (Sieve) Plug-in

- **ISSUE DOV-2803:** Sieve scripts running in IMAPSIEVE or IMAP FILTER=SIEVE context that modify the message, store the message a second time rather than replacing the originally stored unmodified message.
    - FIX: Discard the original unmodified message when Sieve script stores a modified version of the message.
    - Additional feature for IMAPSIEVE: Add new plugin/imapsieve_expunge_discarded setting which causes messages discarded by an IMAPSIEVE script to be expunged immediately, rather than only being marked as "\Deleted" (which is still the default behavior).

- **ISSUE DOV-2932:** IMAPSieve: When a COPY command copies messages from a virtual mailbox, a crash occurs when the source messages originate from more than a single real mailbox: Panic: file imap-sieve-storage.c: line 337 (imap_sieve_add_mailbox_copy_event): assertion failed: (ismt->src_box == NULL || ismt->src_box == src_mail->box)

5.4. Full Text Search (FTS) Plug-in

- **ISSUE DOV-2929:** fs-fts-cache: After failed FTS triplet uploads FTS cache may have ended up in a state where triplets were being uploaded to object storage without being merged. This resulted in a lot of tiny triplets being stored to object storage.

6. Tests

The Dovecot 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.