Release Notes for Dovecot Pro Patch Release v2.3.4.1

Table of Contents

1. Shipped Products and Versions

Dovecot Pro v2.3.4.1
Including Object Storage and Full Text Search Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS/RHEL 6.9, 7.6
- Debian jessie (8.11), stretch (9.7)
- 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

4. Known Issues

- 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.
- Due to on-going changes in Dovecot logging & statistics, event leak warnings may occur in the logs. [DOP-660]
    - Example: "Warning: Event 0x564bde864a00 leaked" may appear in logs.
    - Known situations where these warnings are emitted include Dovecot restarts, typos in Dovecot configuration, and external services (auth or dict) failing to respond.
    - The warnings may repeat, sometimes at a fixed time (e.g. 30 minutes) after the related error (e.g. auth error).
    - These warnings do not affect system performance, and no action is required to address them.
    - These spurious warnings will be resolved in a future release of Dovecot.
- Assert crash may occur on an interrupted APPEND when using Maildir + zlib plugin. [DOP-652]
- `login_proxy_max_disconnect_delay` may cause a panic when using a non-default setting (e.g. imap-login: Panic: io_add(0x1) called twice fd=17, callback=0x7fb039a122f0 -> 0x7fb039a0c8b0). Workaround: remove the setting from Dovecot config or set to the default value (default = 0). [DOV-2648; DOV-2670]
- In some cases, the output from doveadm log errors does not contain user/session information. The log files are unaffected by this. [DOV-2676]
- HTTP storage connection problems can lead to panics (http-client-queue.c: line 518 (http_client_queue_connection_failure): assertion failed: (queue->cur_peer == peer)). [DOP-672]

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.

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.