Release Notes for OX Dovecot Pro Patch Release v2.3.9.4

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.9.4
Built on Dovecot Community Edition Core v2.3.9.3
Including Object Storage (obox) and Full Text Search (FTS) Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS 6.9, 7.7
- RHEL 6.9, 7.4
- Debian stretch (9.12), buster (10)
- Ubuntu 16.04 LTS (xenial), 18.04 LTS (bionic)

Apache Cassandra Driver: v2.13

2. Release Highlights

SECURITY FIXES

This release fixes three security issues. It is urged that all installations of Dovecot newer than 2.3.0 are upgraded to apply the fixes. The issues are summarized below. 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 18 May 2020.

LMTP/Submission crash on empty local part

The LMTP and Submission services crash when the local-part of an address is "" (double quotes). For LMTP, this can only happen if the MTA passes through all mail deliveries to Dovecot and lets Dovecot determine if a user exists.

This issue is present in Dovecot since version 2.3.0.

Workaround:

For submission there is no workaround, but triggering the bug requires valid credentials.

For LMTP, one can implement sufficient filtering on MTA level to prevent mails with such addresses from ending up in LMTP delivery.

CVE-2020-10967; CVSS Score: 5.3 (CVSS3.1:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

LMTP/Submission crash on malformed NOOP

Sending a malformed NOOP command causes a crash in submission, submission-login, or LMTP service. For LMTP, this can only occur if the LMTP service is open to the public (NOT RECOMMENDED) or the local MTA is malicious.

This issue is present in in Dovecot since version 2.3.0.

CVE-2020-10957; CVSS: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Possible LMTP/submission crash on invalid commands

Sending many invalid or unknown commands can cause the server to access freed memory, which can lead to a server crash. This happens when the server closes the connection with a "`421 Too many invalid commands`" error. The bad command limit depends on the service (LMTP or submission) and varies between 10 to 20 bad commands.

This issue is present in in Dovecot since version 2.3.0.

CVE-2020-10958; CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Summary of Highlights

- Fix security issues CVE-2020-10967, CVE-2020-10957, and CVE-2020-10958

3. Upgrade Instructions

No Changes

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.

5. Detailed Changes

5.1. Dovecot Pro Core

- **SECURITY DOV-3846**: lmtp/submission: Issuing the RCPT command with an address that has the empty quoted string as local-part causes the lmtp service to crash. (CVE-2020-10967)

- **SECURITY DOV-3874**: lmtp/submission: A client can crash the server by sending a NOOP command with an invalid string parameter. This occurs particularly for a parameter that doesn't start with a double quote. This applies to all SMTP services, including submission-login, which makes it possible to crash the submission service without authentication. (CVE-2020-10957)

- **SECURITY DOV-3875**: lmtp/submission: Sending many invalid or unknown commands can cause the server to access freed memory, which can lead to a server crash. This happens when the server closes the connection with a "421 Too many invalid commands" error. The bad command limit depends on the service (lmtp or submission) and varies between 10 to 20 bad commands. (CVE-2020-10958)

5.2. Object Storage (obox) Plug-in

No Changes

5.3. Full Text Search (fts) Plug-in

No Changes

5.4. Pigeonhole (sieve) Plug-in

No Changes

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

No Changes

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

No Changes

5.7. 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/.