Release Notes for OX Dovecot Pro Patch Release v2.3.9.3

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro 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 (9.11), buster (10)
- Ubuntu 16.04 LTS (xenial), 18.04 LTS (bionic)

Apache Cassandra Driver: v2.9

2. Release Highlights

This release fixes several vulnerabilities in Dovecot Pro that potentially allow Denial of Service attacks.

These vulnerabilities were discovered internally. OX has no knowledge of these exploits being used as targeted attacks in the wild.

These vulnerabilities will be publicly announced earliest on 2020-02-12. The release notes are, until that date, CONFIDENTIAL and restricted to OX Dovecot Pro customers only.

LMTP/Submission Parsing

LMTP and Submission servers didn't handle partial UTF-8 characters correctly in parameters, resulting in infinite loop taking 100% CPU. This could be used to DoS these services without the need to authenticate.

This is a regression in Dovecot Pro 2.3.9.2 only.

CVE-2020-7046; CVSS Score: 7.5 (CVSS3.1:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7046

Message Snippet/Preview Generation

Message snippet generation may have crashed with large mails that ended with '>'.

This is a security in Dovecot Pro 2.3.9.2 only.

CVE-2020-7957; CVSS Score: 3.1 (CVSS3.1:/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L)

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7957

Retpoline Hardening Flag Removed

For Dovecot Pro 2.3.x, various compiler hardening flags were enabled that focus on enhancing security. Recently, it was discovered that these flags may be responsible for performance degradation as compared with previous versions, and an investigation is currently underway to determine impact.

Initial indications are that the "retpoline" compiler flag, intended to mitigate Spectre Variant 2, causes significant performance penalties. These penalties are platform dependent, and early testing identifies Dovecot's indexer-worker as the most affected process.

Given this large performance penalty, and research that indicates that this mitigation should already be sufficiently handled by modern kernels, it was decided to remove this hardening flag for this release of Dovecot Pro.

Note that investigation is ongoing, and additional compiler hardening flag changes may occur in future versions of Dovecot Pro depending on the results.

Summary of Highlights

- Fix CVE-2020-7046, CVE-2020-7957
- Removed retpoline hardening compiler flag

3. Upgrade Instructions

None

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-3743 [CVE-2020-7957]**: Message snippet generation may have crashed with large mails that ended with '>'. v2.3.9 regression.
- **SECURITY DOV-3744 [CVE-2020-7046]**: LMTP and Submission servers didn't handle partial UTF-8 characters correctly in parameters, resulting in infinite loop taking 100% CPU. This could be used to DoS the submission service without logging in. Regression in v2.3.9.

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

- **SECURITY DOV-3742**: Utimaco X1 management protocol requests didn't handle invalid UTF-8 properly, potentially resulting in crashes or out-of-memory. The X1 requests typically come from a trusted source though, so this may not be possible to exploit.

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/.