Release Notes for OX Dovecot Pro Patch Release v2.3.21.1

Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.21.1
Built on Dovecot Community Edition Core v2.3.21
Including Object Storage (obox) and Full Text Search (fts-dovecot) Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS 7.9
- RHEL 7.4, 8.2
- Debian buster (10), bullseye (11)
- Ubuntu 18.04 LTS (bionic), 20.04 LTS (focal)
    - Note: Future support for Ubuntu 22.04 LTS (jammy) is unlikely for v2.3.x due to its dependency on OpenSSL 3.0.

Apache Cassandra Driver: v2.16.2

2. Release Highlights

This is a security release of the OX Dovecot Pro v2.3 branch, which also contains bug fixes.

SECURITY FIXES

This release fixes two security issues. **It is recommended that installations of OX Dovecot Pro that are directly affected by these issues upgrade to this version as soon as possible.** Further details will be made available when the issues are disclosed to the public.

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 14 August 2024.

Address Header Parsing (CPU Usage)

Having a large number of address headers (From, To, Cc, Bcc, etc.) becomes excessively CPU intensive. With 100,000 header lines CPU usage is 12 seconds, and in a production environment we observed 500,000 header lines taking 18 minutes to parse.

Since this behavior can be triggered by external actors sending emails to a victim, this is a security issue. The main problem is that each header line's address is added to the end of a linked list. This is done by walking the whole linked list, which becomes more inefficient the more addresses there are.

Workaround:

- Implement restrictions on address headers on MTA (and AV/AS) component preceding Dovecot. This is recommended independent of this security issue, as these messages may be difficult to handle on user clients as well.

CVE-2024-23184; CVSS Score: 5.0
(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N)

Address Header Parsing (Memory Usage)

The message-parser normally reads reasonably sized chunks of the message. However, when it feeds them to message-header-parser, it starts building up "full_value" buffer out of the smaller chunks. The “full_value” buffer has no size limit, so large headers can cause large memory usage. It doesn't matter whether it's a single long header line, or a single header split into multiple lines.

This bug exists in all Dovecot versions.

Incoming mails typically have some size limits set by MTA, so even the largest possible header size may still fit into Dovecot's vsz_limit. Thus, attackers probably can't DoS a victim user with this technique. A user could APPEND larger mails though, allowing them to DoS themselves (although it may cause some memory issues for the Dovecot backend in general).

Workaround:

- Implement restrictions on address headers or message size on MTA (and AV/AS) component preceding Dovecot. This is recommended independent of this security issue, as these messages may be difficult to handle on user clients as well. (It is expected that most installations already have some incoming message size limit, enforced via MTAs, so it is likely this is not a serious vulnerability in existing setups.)

CVE-2024-23185; CVSS Score: 7.5
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

3. Upgrade Information

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. OX Dovecot Pro Core

- **SECURITY DOV-6880**: A large number of address headers in email resulted in excessive CPU usage.

- **SECURITY DOV-6881**: Abnormally large email headers are now truncated/discarded, with a limit of 10MB on a single header and 50MB for all the headers of all the parts of an email.

- **ISSUE DOV-6877**: If passdb oauth2 was not first, crash would occur when authentication fails.

5.2. Object Storage (obox) Plugin

No Changes.

5.3. Full Text Search (fts-dovecot) Plugin

No Changes.

5.4. Pigeonhole (sieve) Plugin

No Changes.

5.5. Other Plugins

5.5.1. Intercept (intercept) Plugin

- **IMPROVEMENT DOV-6875**: Support UUID matching between Utimaco X1 and X3.
- **ISSUE DOV-6876**: login_intercept didn't handle STARTTLS correctly. It was writing the encrypted network traffic into the intercept files.

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/.