Release Notes for OX Dovecot Pro Patch Release v2.3.5.1

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.5.1
Including Object Storage (obox) and Full Text Search (FTS) Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS/RHEL 6.9, 7.6
- Debian jessie (8.11), stretch (9.7)
- Ubuntu 16.04 LTS, 18.04 LTS

2. Security Advisory

This release fixes a vulnerability in Dovecot that potentially allows local root privilege escalation or executing arbitrary code in Dovecot process context. This can occur if either FTS or POP3-UIDL features are enabled.

Direct write access to Dovecot index files is required, via either storage or, for obox, access to a user's index files contained on a backend in the metacache. Therefore, this vulnerability requires local shell access to be easily exploitable.

Since v2.3.0, stack protection and other binary hardening has been used when generating OX Dovecot Pro packages which makes this issue more difficult to exploit in practice.

This vulnerability was found internally. OX has no knowledge of this exploit being used in the wild.

Customers running OX Dovecot Pro generally only provide admin access to the backends and storage. Without external user access to these systems, OX is not aware of any method to exploit this vulnerability remotely. However, as with any security vulnerability, OX recommends upgrading to the fixed version as soon as possible.

This vulnerability will be publicly announced on Thursday, 28 March 2019.

CVE-2019-7524; CVSS Score: 8.8
(3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C)

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7524

3. 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.
- 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)). [DOV-2786]

4. Detailed Changes

4.1. Dovecot Pro Core

- **SECURITY DOV-2964 [CVE-2019-7524]:** Missing input buffer size validation leads into arbitrary buffer overflow when reading fts or pop3 uidl header from dovecot index. Exploiting this requires direct write access to the index files or object storage.

5. 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.