DOVECOT

Release Notes for OX Dovecot Pro Patch Release v2.3.5.2

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.5.2
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 regarding JSON encoding. Invalid UTF-8 sequences that is passed through Dovecot's internal JSON encoder will cause a crash due to an explicit assert contained in the code to capture this kind of invalid input.

There are two locations in OX Dovecot Pro where this issue can be triggered:

1. Authentication policy is being used (i.e. OX Abuse Shield). If authentication policy is active, authentication usernames or passwords will be JSON encoded before sending to the policy service. Invalid UTF-8 characters in the username will cause the authentication process to crash. This allows a remote attacker to potentially cause denial of service on the Dovecot system by continually crashing the authentication process.
2. OX Push Notifications encode various message data via JSON before sending to the remote endpoint. If a message contains invalid UTF-8 data in certain headers, this would cause the push notification code to crash. Generally, push notifications are configured to trigger during message delivery, typically in the LMTP process.

This vulnerability was introduced in OX Dovecot Pro v2.3.0, when an assert was added to trigger a panic when invalid data was detected. Earlier versions, v2.2.x, will forward the invalid sequences as is. Therefore, APIs receiving them should be checked for possible issues dealing with such sequences.

To work around these issues:

1. Disable Authentication policy.
2. Do not load the OX push notification driver.

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

This vulnerability will be publicly announced on Thursday, 18 April 2019.

CVE-2019-10691; CVSS Score: 7.5 (CVSS:3.0/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-2019-10691

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-3173 [CVE-2019-10691]:** Invalid UTF-8 sequences cause crash in JSON encoder when auth policy or OX push notification is used: Panic: file json-parser.c: line 825 (json_append_escaped_data): assertion failed: (bytes > 0 && uni_is_valid_ucs4(chr))

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.