Open-Xchange Security Advisory 2019-03-28

Product: Dovecot
Vendor: OX Software GmbH

Internal reference: DOV-2964 (Bug ID)
Vulnerability type: CWE-120
Vulnerable version: 2.0.14 - 2.3.5
Vulnerable component: fts, pop3-uidl-plugin
Report confidence: Confirmed
Researcher credits: Found in internal testing
Solution status: Fixed by Vendor
Fixed version: 2.3.5.1, 2.2.36.3
Vendor notification: 2019-02-05
Solution date: 2019-03-21
Public disclosure: 2019-03-28
CVE reference: CVE-2019-7524
CVSS: 3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C (8.8)

Vulnerability Details:

When reading FTS or POP3-UIDL header from dovecot index, the input buffer size is not bound, and data is copied to target structure causing stack overflow.

Risk:

This can be used for local root privilege escalation or executing arbitrary code in dovecot process context. This requires ability to directly modify dovecot indexes.

Steps to reproduce:

1. Produce dovecot.index.log entry that creates an FTS header which has more than 12 bytes of data.
2. Trigger dovecot indexer-worker or run doveadm index.
3. Dovecot will crash.

Mitigations:

Since 2.3.0 dovecot has been compiled with stack smash protection, ASLR, read-only GOT tables and other techniques that make exploiting this bug much harder.

Solution:

Operators should update to the latest Patch Release. The only workaround is to disable FTS and pop3-uidl plugin.