Multiple vulnerabilities in Dovecot IMAP server

From: Aki Tuomi <aki.tuomi () dovecot fi>
Date: Mon, 18 May 2020 15:03:33 +0300 (EEST)

Dear subscribers,

we are sending notifications for three vulnerabilities,

- CVE-2020-10957
- CVE-2020-10958
- CVE-2020-10967

Please find them below

Aki Tuomi
Open-Xchange Oy

Open-Xchange Security Advisory 2020-05-18

Product: Dovecot
Vendor: OX Software GmbH

Internal reference: DOV-3784
Vulnerability type: NULL pointer dereference (CWE-476)
Vulnerable version: 2.3.0 - 2.3.10
Vulnerable component: submission, lmtp
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 2.3.10.1
Researcher credits: Philippe Antoine (Catena Cyber)
Vendor notification: 2020-03-24
Solution date: 2020-04-02
Public disclosure: 2020-05-18
CVE reference: CVE-2020-10957
CVSS: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Vulnerability Details:
Sending malformed NOOP command causes crash in submission, submission-login or lmtp service.

Risk:
Remote attacker can keep submission-login service down, causing denial of service attack. For lmtp the risk is neglible, as lmtp is usually behind a trusted MTA.

Steps to reproduce:
Send ``NOOP EE"FY`` to submission port, or similarly malformed command.

Solution:
Upgrade to fixed version.

Open-Xchange Security Advisory 2020-05-18

Product: Dovecot IMAP server
Vendor: OX Software GmbH

Internal reference: DOV-3875
Vulnerability type: Improper handling of input data (CWE-20)
Vulnerable version: 2.3.0 - 2.3.10
Vulnerable component: submission, lmtp
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 2.3.10.1
Researcher credits: Philippe Antoine (Catena Cyber)
Vendor notification: 2020-03-23
Solution date: 2020-04-02
Public disclosure: 2020-05-18
CVE reference: CVE-2020-10958
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Vulnerability Details:

Sending command followed by sufficient number of newlines triggers a use-after-free bug that might crash submission-login, submission or lmtp service.

Risk:

Remote attacker can keep submission-login service down, causing denial of service attack. For lmtp the risk is neglible, as lmtp is usually behind a trusted MTA.

Steps to reproduce:

This can be currently reproduced with ASAN or Valgrind. Reliable way to crash has not yet been discovered.

Solution:

Upgrade to fixed version.

Open-Xchange Security Advisory 2020-05-18

Product: Dovecot
Vendor: OX Software GmbH

Internal reference: DOV-1745
Vulnerability type: Improper input validation (CWE-20)
Vulnerable version: 2.3.0 - 2.3.10
Vulnerable component: submission, lmtp
Report confidence: Confirmed
Solution status: Fixed by Vendor
Fixed version: 2.3.10.1
Researcher credits: mailbox.org
Vendor notification: 2020-03-20
Solution date: 2020-04-02
Public disclosure: 2020-05-18
CVE reference: CVE-2020-10967
CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

Vulnerability Details:
Sending mail with empty quoted localpart causes submission or lmtp component
to crash.

Risk:
Malicious actor can cause denial of service to mail delivery by repeatedly
sending mails with bad sender or recipient address.

Steps to reproduce:
Send mail with envelope sender or recipient as ``<""@example.org>``.

Workaround:
For submission there is no workaround, but triggering the bug requires valid
credentials.
For lmtp, one can implement sufficient filtering on MTA level to prevent mails
with such addresses from ending up in LMTP delivery.

Solution:
Upgrade to fixed version.

Attachment: signature.asc
Description:

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

By Date By Thread

Current thread:

Multiple vulnerabilities in Dovecot IMAP server *Aki Tuomi (May 19)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License