[Dovecot-news] CVE-2020-7957: Specially crafted mail can crash snippet generation

Aki Tuomi aki.tuomi at dovecot.fi
Wed Feb 12 14:05:06 EET 2020

- Previous message: [Dovecot-news] Dovecot v2.3.9.3 released
- Next message: [Dovecot-news] CVE-2020-7046: Truncated UTF-8 can be used to DoS submission-login and lmtp processes
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Open-Xchange Security Advisory 2020-02-12

Affected product: Dovecot Core
Internal reference: DOV-3743 (JIRA ID)
Vulnerability type: Improper Input Validation (CWE-30)
Vulnerable version: 2.3.9
Vulnerable component: lmtp, imap
Fixed version: 2.3.9.3
Report confidence: Confirmed
Solution status: Fixed
Researcher credits: Open-Xchange oy
Vendor notification: 2020-01-14
CVE reference: CVE-2020-7957
CVSS: 3.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L)

Vulnerability Details:

Snippet generation crashes if:

     message is large enough that message-parser returns multiple body
blocks
    The first block(s) don't contain the full snippet (e.g. full of
whitespace)
    input ends with '>'

Risk:

Sending specially crafted email can cause mailbox to have permanently
unaccessible mail, or the mail can be stuck in delivery.

Solution:

Upgrade to 2.3.9.3


-------------- next part --------------
A non-text attachment was scrubbed...
Name: signature.asc
Type: application/pgp-signature
Size: 488 bytes
Desc: OpenPGP digital signature
URL: <https://dovecot.org/pipermail/dovecot-news/attachments/20200212/9c060974/attachment.sig>
```

- Previous message: [Dovecot-news] Dovecot v2.3.9.3 released
- Next message: [Dovecot-news] CVE-2020-7046: Truncated UTF-8 can be used to DoS submission-login and lmtp processes
- **Messages sorted by:** [date] [thread] [subject] [author]

More information about the Dovecot-news mailing list