muttmua / **mutt** Public

Code | Pull requests | Actions | Projects | Security and quality | Insights

Commit `fdc04a1`

kevin8t8 committed 2 weeks ago

```
Fix infinite loop in gpgme data_object_to_stream().

The code was not properly checking for a -1 return value in the read,
leading to an infinite loop, and printing past the buffer value to the
stream.

Thanks to evilrabbit@tutamail.com for the security report.

Reviewed-by: Alejandro Colomar <alx@kernel.org>
```

master · mutt-2-3-2-rel

1 parent ebfa296 commit fdc04a1

1 file changed +1 -1

Top

Filter files…

crypt-gpgme.c

Search within code

crypt-gpgme.c

```
@@ -742,7 +742,7 @@ static int data_object_to_stream (gpgme_data_t data,
FILE *fp)
742 742         return -1;
743 743       }
744 744
745       -   while ((nread = gpgme_data_read(data, buf, sizeof (buf))))
      745 +   while ((nread = gpgme_data_read(data, buf, sizeof (buf))) > 0)
746 746       {
```

```
747   747          /* fixme: we are not really converting CRLF to LF but just
748   748             skipping CR. Doing it correctly needs a more complex logic */
```

Comments 0

Please sign in to comment.