muttmua / **mutt** Public

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

Commit ebfa296

kevin8t8 committed 2 weeks ago

```
Fix NULL dereference in show_sig_summary().

Inside show_one_sig_status(), if the error code is GPG_ERR_NO_PUBKEY,
key is NULL.  However, show_sig_summary() doesn't check for a NULL key
before dereferencing for the "key expired" case.

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

Thanks to Alejandro Colomar for his review and suggestion to keep the
ternary operator.

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

1 parent 519d1b9 commit ebfa296

1 file changed +1 -1

Top

Filter files...

crypt-gpgme.c

Search within code

crypt-gpgme.c

```
@@ -1425,7 +1425,7 @@ static int show_sig_summary (unsigned long sum,
1425 1425
1426 1426       if ((sum & GPGME_SIGSUM_KEY_EXPIRED))
1427 1427         {
1428      -        time_t at = key->subkeys->expires ? key->subkeys->expires : 0;
     1428 +        time_t at = (key && key->subkeys) ? key->subkeys->expires : 0;
```

```
1429  1429          if (at)
1430  1430            {
1431  1431              state_puts (_("Warning: The key used to create the "
```

Comments 0

Please sign in to comment.