muttmua / **mutt** Public

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

Commit 834c5a2

kevin8t8 committed 2 weeks ago

```
Fix IMAP auth_cram MD5 digest of secret to use memcpy().

For a secret longer than MD5_BLOCK_LEN, an MD5 digest is used instead.
However, mutt was incorrectly using strfcpy() instead of memcpy() on
the raw binary value returned by md5_buffer in hash_passwd.  If
hash_passwd contained an '\0' it would result in the value being
truncated.

Additionally, the strfcpy was truncating the hash_passwd by one byte
regardless, due to passing a "size" of MD5_DIGEST_LEN when the data
itself was length MD5_DIGEST_LEN.

This likely hasn't been a reported issue because:
1. CRAM-MD5 is not used much anymore
2. Most people likely don't have a password length greater than 64
   bytes.

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

master · mutt-2-3-2-rel

1 parent 12f54fe commit 834c5a2

1 file changed +1 -1

Top

Filter files…

imap

auth_cram.c

Search within code

imap/auth_cram.c

```
@@ -149,7 +149,7 @@ static void hmac_md5 (const char* password, char*
challenge,
149 149     if (secret_len > MD5_BLOCK_LEN)
150 150     {
151 151       md5_buffer (password, secret_len, hash_passwd);
152     -     strfcpy ((char*) secret, (char*) hash_passwd, MD5_DIGEST_LEN);
    152 +     memcpy(secret, hash_passwd, MD5_DIGEST_LEN);
153 153       secret_len = MD5_DIGEST_LEN;
154 154     }
155 155     else
```

Comments 0

Please sign in to comment.