4

CVE-2022-35260: .netrc parser out-of-bounds access

Share:

TIMELINE

kurohiro submitted a report to curl. Oct 3rd (2 months ago)

Summary:

Curl expects the .netrc file to have space characters. So if there is no space character, it will do an out-of-bounds read and a 1-byte out-of-bounds write.
This can happen multiple times depending on the state of the memory.

Steps To Reproduce:

```
curl --netrc-file .netrc test.local
```

".netrc" is attached.
The content is 'a' for 4095 bytes.
Depending on memory conditions, even single-byte files can cause problems.

It's not exactly just spaces and newlines.
The condition is that the .netrc file does not contain characters for which ISSPACE() returns true (so it is also a condition that there is no line feed code).
There is a problem with parsenetrc() in lib/netrc.c.
parsenetrc() has the following loop.

Code 746 Bytes Wrap lines Copy Download

```
1       while(!done && fgets(netrcbuffer, netrcbuffsize, file)) {
2         char *tok;
3         char *tok_end;
4         bool quoted;
5         if(state == MACDEF) {
6           if((netrcbuffer[0] == '\n') || (netrcbuffer[0] == '\r'))
7             state = NOTHING;
8           else
9             continue;
10         }
11         tok = netrcbuffer;
12         while(tok) {
13           while(ISSPACE(*tok))
14             tok++;
15           /* tok is first non-space letter */
16           if(!*tok || (*tok == '#'))
17             /* end of line or the rest is a comment */
18             break;
19
20           /* leading double-quote means quoted string */
21           quoted = (*tok == '\"');
22
23           tok_end = tok;
24           if(!quoted) {
25             while(!ISSPACE(*tok_end))
26               tok_end++;
27             *tok_end = 0;
28           }
```

The 'a' and the terminating character '\0' in the .netrc file are characters for which ISSPACE() returns false, so while on line 25 is true(!false).
This causes an out-of-bounds read.
Also, line 27 is an out-of-bounds write. (1 byte for '\0).

Remediation ideas:

I think it would be better to include the condition that *tok is not NULL in the while statement.

Impact

Application crash plus other as yet undetermined consequences.

1 attachment:
F1967256: .netrc