3 **CVE-2021-22923: Metalink download sends credentials**

Share:

TIMELINE

nyymi submitted a report to curl. May 30th (2 years ago)

Summary:

When compiled `--with-libmetalink` and used with `--metalink` and `--user` curl will use the credentials for any further transfers performed. This includes different hosts and protocols, even ones without transport layer security such as `http` and `ftp` . As a result the credentials only intended for the target site may end up being sent to outside hosts, and without transport layer security, and may be intercepted by attackers in man in the middle network position.

For example HTTP redirects will not leak the credentials to other hosts unless if `--location-trusted` is used, thus this is unexpected and insecure behaviour.

Steps To Reproduce:

1. Configure libcurl `--with-libmetalink` and build libcurl
2. Have metalinktest.xml with `<url>` referencing data on different host than testsite and using `http` protocol
3. Execute: `curl --metalink --user professor:Joshua https://testsite/metalinktest.xml`

The credentials can be seen by the target host and anyone in man in the middle position:
`Authorization: Basic cHJvZmVzc29yOkpvc2h1YQ==`

Remarks

CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) might be a more accurate CWE.

Fix

- Perhaps `--location-trusted` should be extended to apply to `--metalink` as well

Impact

Leak of credentials to unauthorized parties§

dgustafsson curl staff posted a comment. May 31st (2 years ago)

Thank you for your report!

We will take some time and investigate your reports and get back to you with details and possible follow-up questions as soon as we can!

bagder curl staff posted a comment. May 31st (2 years ago)

This might actually often be exactly what the user wants and expects but it may also not be. I don't think `--location-trusted` should be involved, since that's about following redirects and this isn't about redirects.

nyymi posted a comment. May 31st (2 years ago)

Hmm. It also seems that `--user professor:Joshua` overrides any credentials specified in the URLs in the XML. Say XML with `<url>http://foo:bar@testsite:9999</url>` results in `Authorization: Basic cHJvZmVzc29yOkpvc2h1YQ==` (professor:Joshua) is sent to the server.
I'm not sure if this is what should really happen here... This is a bit unspecified territory again. This is again something that metalink RFC should have specified I think.

bagder curl staff updated the severity from High to Medium. Jun 11th (2 years ago)

bagder curl staff changed the status to ○ **Triaged**. Jun 11th (2 years ago)

bagder curl staff changed the report title from **metalink download always sending credentials regardless of --location-trusted** to **metalink download sends on credentials**. Jun 11th (2 years ago)

bagder curl staff posted a comment. Jun 18th (about 1 year ago)

First take:

Metalink download sends credentials

Project curl Security Advisory, July 21th 2021 -
Permalink

VULNERABILITY

When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened.

We are not aware of any exploit of this flaw.

INFO

This flaw exists only in the curl tool. libcurl is not affected.

This flaw has existed in curl since commit
b5fdbe848bc3d in curl
7.27.0, released on July 27, 2012.

CWE-522: Insufficiently Protected Credentials

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 7.27.0 to and including 7.77.0
- Not affected versions: curl < 7.27.0 and curl >= 7.78.0

Also note that libcurl is used by many applications, and not always advertised as such.

THE SOLUTION

curl has completely removed the metalink feature as of 7.78.0

The fix for earlier versions is to rebuild curl with the metalink support switched off!

RECOMMENDATIONS

A - Upgrade curl to version 7.78.0

B - Make sure you do not use metalink with curl

C - Disable metalink in your build

TIMELINE

This issue was reported to the curl project on May 30, 2021.

This advisory was posted on Jul 21, 2021.

CREDITS

This issue was reported by Harry Sintonen. Patched by Daniel Stenberg.

Thanks a lot!

1 attachment:
F1343750: CVE-2021-JJJJJ.md

nyymi posted a comment. Jun 18th (about 1 year ago)

Looking good. In this particular advisory "Also note that libcurl is used by many applications, and not always advertised as such." could be omitted in this advisory as the issue only applies to `curl` command itself.

Technically this is of course correct, but it isn't relevant in this specific case.

dfandrich curl staff posted a comment. Jun 18th (about 1 year ago)

I would make it explicit in the "The Solution" section by adding a line like "No fix for this flaw will be produced by the curl project." so nobody wastes time looking for a patch that doesn't exist.

bagder curl staff posted a comment. Jun 18th (about 1 year ago)

Thanks both, I'm updating my local copy accordingly.

bagder curl staff updated CVE reference to CVE-2021-22923. Jun 28th (about 1 year ago)

bagder curl staff changed the report title from **metalink download sends on credentials** to **CVE-2021-22923: Metalink download sends credentials**. Jun 28th (about 1 year ago)

curl rewarded nyymi with a **$700** bounty. Jun 30th (about 1 year ago)

The curl security team has decided to reward hacker @nyymi with the amount of 700 USD for finding and reporting this issue. Many thanks for your great work!

bagder curl staff closed the report and changed the status to **Resolved**. Jul 21st (about 1 year ago)

bagder curl staff requested to disclose this report. Jul 21st (about 1 year ago)

nyymi agreed to disclose this report. Jul 21st (about 1 year ago)

This report has been disclosed. Jul 21st (about 1 year ago)