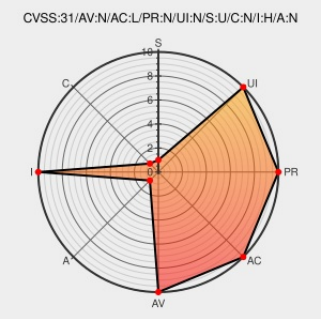
CVE-2022-27780

Published on: Not Yet Published

Last Modified on: 06/22/2022 01:48:00 PM UTC

CVE-2022-27780

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Curl from Haxx contain the following vulnerability:

The curl URL parser wrongly accepts percent-encoded URL separators like '/'when decoding the host name part of a URL, making it a *different* URL usingthe wrong host name when it is later retrieved.For example, a URL like `http://example.com%2F127.0.0.1/`, would be allowed bythe parser and get transposed into `http://example.com/127.0.0.1/`. This flawcan be used to circumvent filters, checks and more.

CVE-2022-27780 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
June 2022 Libcurl Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20220609-0009/

HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1553841

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

198780 Ubuntu Security Notification for curl Vulnerabilities (USN-5412-1)

282696 Fedora Security Update for curl (FEDORA-2022-d15a736748)

502213 Alpine Linux Security Update for curl

502408 Alpine Linux Security Update for curl

690868 Free Berkeley Software Distribution (FreeBSD) Security Update for curl (11e36890-d28c-11ec-a06f-d4c9ef517024)

902169 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (9895)

902174 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (9909)

902387 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (9909-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haxx	Curl	All	All	All	All

cpe:2.3:a:haxx:curl:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@bagder	CVE-2022-27778: removes wrong file on error CVE-2022-27779: cookie for trailing dot TLD CVE-2022-27780: percent-enc… twitter.com/i/web/status/1…	2022-05-11 06:44:32
@sidfm_jp	cURL に URL の解釈を誤る問題 (CVE-2022-27780) [42170] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2022-05-12 08:00:06
@CVEreport	cve.report/CVE-2022-27780 The curl URL parser wrongly accepts percent-encoded URL separators like '/'when decoding t… twitter.com/i/web/status/1…	2022-06-02 16:36:01
@LinInfoSec	Curl - CVE-2022-27780: hackerone.com/reports/1553841	2022-06-02 17:00:13
/r/opnsense	already curl-7.83.0 is vulnerable:	2022-05-13 21:52:27

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report