



stale custom cookie host causes cookie leak

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-6276
State	PUBLISHED
Assigner	curl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-13 13:01:56 UTC
Updated	2026-05-14 14:21:06 UTC
Description	Using libcurl, when a custom `Host:` header is first set for an HTTP request and a second request is subsequently done usi

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.000170000 probability, percentile 0.044100000 (date 2026-05-17)

Problem Types: CWE-319 | CWE-346 Origin Validation Error

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Curl	Curl	affected 8.19.0 8.19.0 semver	Not specified
CNA	Curl	Curl	affected 8.18.0 8.18.0 semver	Not specified
CNA	Curl	Curl	affected 8.17.0 8.17.0 semver	Not specified
CNA	Curl	Curl	affected 8.16.0 8.16.0 semver	Not specified
CNA	Curl	Curl	affected 8.15.0 8.15.0 semver	Not specified
CNA	Curl	Curl	affected 8.14.1 8.14.1 semver	Not specified
CNA	Curl	Curl	affected 8.14.0 8.14.0 semver	Not specified
CNA	Curl	Curl	affected 8.13.0 8.13.0 semver	Not specified
CNA	Curl	Curl	affected 8.12.1 8.12.1 semver	Not specified
CNA	Curl	Curl	affected 8.12.0 8.12.0 semver	Not specified
CNA	Curl	Curl	affected 8.11.1 8.11.1 semver	Not specified
CNA	Curl	Curl	affected 8.11.0 8.11.0 semver	Not specified
CNA	Curl	Curl	affected 8.10.1 8.10.1 semver	Not specified
CNA	Curl	Curl	affected 8.10.0 8.10.0 semver	Not specified
CNA	Curl	Curl	affected 8.9.1 8.9.1 semver	Not specified
CNA	Curl	Curl	affected 8.9.0 8.9.0 semver	Not specified
CNA	Curl	Curl	affected 8.8.0 8.8.0 semver	Not specified
CNA	Curl	Curl	affected 8.7.1 8.7.1 semver	Not specified
CNA	Curl	Curl	affected 8.7.0 8.7.0 semver	Not specified
CNA	Curl	Curl	affected 8.6.0 8.6.0 semver	Not specified
CNA	Curl	Curl	affected 8.5.0 8.5.0 semver	Not specified
CNA	Curl	Curl	affected 8.4.0 8.4.0 semver	Not specified
CNA	Curl	Curl	affected 8.3.0 8.3.0 semver	Not specified
CNA	Curl	Curl	affected 8.2.1 8.2.1 semver	Not specified

CNA	Curl	Curl	affected 8.2.0 8.2.0 semver	Not specified
CNA	Curl	Curl	affected 8.1.2 8.1.2 semver	Not specified
CNA	Curl	Curl	affected 8.1.1 8.1.1 semver	Not specified
CNA	Curl	Curl	affected 8.1.0 8.1.0 semver	Not specified
CNA	Curl	Curl	affected 8.0.1 8.0.1 semver	Not specified
CNA	Curl	Curl	affected 8.0.0 8.0.0 semver	Not specified
CNA	Curl	Curl	affected 7.88.1 7.88.1 semver	Not specified
CNA	Curl	Curl	affected 7.88.0 7.88.0 semver	Not specified
CNA	Curl	Curl	affected 7.87.0 7.87.0 semver	Not specified
CNA	Curl	Curl	affected 7.86.0 7.86.0 semver	Not specified
CNA	Curl	Curl	affected 7.85.0 7.85.0 semver	Not specified
CNA	Curl	Curl	affected 7.84.0 7.84.0 semver	Not specified
CNA	Curl	Curl	affected 7.83.1 7.83.1 semver	Not specified
CNA	Curl	Curl	affected 7.83.0 7.83.0 semver	Not specified
CNA	Curl	Curl	affected 7.82.0 7.82.0 semver	Not specified
CNA	Curl	Curl	affected 7.81.0 7.81.0 semver	Not specified
CNA	Curl	Curl	affected 7.80.0 7.80.0 semver	Not specified
CNA	Curl	Curl	affected 7.79.1 7.79.1 semver	Not specified
CNA	Curl	Curl	affected 7.79.0 7.79.0 semver	Not specified
CNA	Curl	Curl	affected 7.78.0 7.78.0 semver	Not specified
CNA	Curl	Curl	affected 7.77.0 7.77.0 semver	Not specified
CNA	Curl	Curl	affected 7.76.1 7.76.1 semver	Not specified
CNA	Curl	Curl	affected 7.76.0 7.76.0 semver	Not specified
CNA	Curl	Curl	affected 7.75.0 7.75.0 semver	Not specified
CNA	Curl	Curl	affected 7.74.0 7.74.0 semver	Not specified
CNA	Curl	Curl	affected 7.73.0 7.73.0 semver	Not specified
CNA	Curl	Curl	affected 7.72.0 7.72.0 semver	Not specified
CNA	Curl	Curl	affected 7.71.1 7.71.1 semver	Not specified
CNA	Curl	Curl	affected 7.71.0 7.71.0 semver	Not specified

References

Reference	Source	Link	Tags
hackerone.com/reports/3671818	134c704f-9b21-4f2e-91b3-4a467353bcc0	hackerone.com	Exploit, Issue Tracking
curl.se/docs/CVE-2026-6276.json	2499f714-1537-4658-8207-48ae4bb9eae9	curl.se	Product
www.openwall.com/lists/oss-security/2026/04/29/13	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List, Third Party
curl.se/docs/CVE-2026-6276.html	2499f714-1537-4658-8207-48ae4bb9eae9	curl.se	Patch, Vendor Advisory

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Muhamad Arga Reksapati (en)

CNA: Daniel Stenberg (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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