



CVE-2016-5420

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-5420
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-10 14:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might all

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

EPSS: 0.010860000 probability, percentile 0.780540000 (date 2026-05-12)

Problem Types: CWE-285 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

High

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Haxx	Libcurl	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
CPU Oct 2018	af854a3c
[SECURITY] Fedora 24 Update: curl-7.47.1-6.fc24 - package-announce - Fedora Mailing-Lists	af854a3c
[R7] LCE 4.8.1 Fixes Multiple Vulnerabilities - Security Advisory Tenable™	af854a3c
openSUSE-SU-2016:2379-1: moderate: Security update for curl	af854a3c
curl - Re-using connections with wrong client cert	af854a3c
Red Hat Customer Portal	af854a3c
Red Hat Customer Portal	af854a3c

Red Hat Customer Portal	af854a3d
USN-3048-1: curl vulnerabilities Ubuntu	af854a3d
cURL/libcurl Certificate Reuse Bug Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker	af854a3d
Android Security Bulletin—December 2016 Android Open Source Project	af854a3d
cURL/libcurl TLS Connection Reuse Bug Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker	af854a3d
Red Hat Customer Portal	af854a3d
openSUSE-SU-2016:2227-1: moderate: Security update for curl	af854a3d
[SECURITY] Fedora 23 Update: curl-7.43.0-8.fc23 - package-announce - Fedora Mailing-Lists	af854a3d
cURL/libcURL CVE-2016-5420 Certificate Validation Security Bypass Vulnerability	af854a3d
cURL: Multiple vulnerabilities (GLSA 201701-47) — Gentoo security	af854a3d
Debian -- Security Information -- DSA-3638-1 curl	af854a3d
The Slackware Linux Project: Slackware Security Advisories	af854a3d
[SECURITY] Fedora 24 Update: curl-7.47.1-6.fc24 - package-announce - Fedora Mailing-Lists	MITRE
[SECURITY] Fedora 23 Update: curl-7.43.0-8.fc23 - package-announce - Fedora Mailing-Lists	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 500111 Alpine Linux Security Update for curl
- 503766 Alpine Linux Security Update for curl
- 710385 Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201701-47)

© [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](#)