



CVE-2016-8623

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

Summary

CVE	CVE-2016-8623
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-01 06:29:00 UTC
Updated	2023-11-07 02:36:00 UTC
Description	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
1388388 – (CVE-2016-8623) CVE-2016-8623 curl: Use-after-free via shared cookies
[bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
cURL/libcURL CVE-2016-8623 Information Disclosure Vulnerability
Pony Mail!
[bookkeeper-issues] 20210629 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade
CPU Oct 2018
curl.haxx.se/CVE-2016-8623.patch
cURL/libcurl Multiple Bugs Let Remote Users Inject Cookies, Reuse Connections, and Execute Arbitrary Code and Let Local Users Obtain Po
cURL: Multiple vulnerabilities (GLSA 201701-47) — Gentoo security

curl - Use-after-free via shared cookies

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500114 Alpine Linux Security Update for curl

503769 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](#)