



CVE-2017-2629

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

Summary

CVE	CVE-2017-2629
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-27 19:29:00 UTC
Updated	2019-10-09 23:26:00 UTC
Description	curl before 7.53.0 has an incorrect TLS Certificate Status Request extension feature that asks for a fresh proof of the server's certificate.

Risk And Classification

Problem Types: CWE-295

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
1425746 – (CVE-2017-2629) CVE-2017-2629 curl: SSL_VERIFYSTATUS ignored
cURL: Certificate validation error (GLSA 201703-04) — Gentoo security
cURL OCSP Stapling Verification Bug Lets Remote Users Bypass CURLOPT_SSL_VERIFYSTATUS Security Restrictions on the Target System
cURL/libcURL CVE-2017-2629 TLS Certificate Validation Security Bypass Vulnerability
curl - SSL_VERIFYSTATUS ignored
[R1] LCE 5.0.1 Fixes Two Third-party Library Vulnerabilities - Security Advisory Tenable™
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500116	Alpine Linux Security Update for curl
503771	Alpine Linux Security Update for curl
710505	Gentoo Linux cURL Certificate validation error Vulnerability (GLSA 201703-04)

© [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](#)