



CVE-2017-7468

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

Summary

CVE	CVE-2017-7468
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-16 13:29:00 UTC
Updated	2019-10-09 23:29:00 UTC
Description	In curl and libcurl 7.52.0 to and including 7.53.1, libcurl would attempt to resume a TLS session even if the client certificate

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- [curl - TLS session resumption client cert bypass](#)
- [cURL: Multiple vulnerabilities \(GLSA 201709-14\) — Gentoo Security](#)
- [cURL/libcurl TLS Session Resumption Client Certificate Bug Lets Remote Users Bypass Security Restrictions on the Target System - Security](#)
- [1443381 – \(CVE-2017-7468\) CVE-2017-7468 curl: TLS session resumption client cert bypass](#)
- [cURL/libcURL CVE-2017-7468 Remote Security Bypass Vulnerability](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500118](#) Alpine Linux Security Update for curl

[503773](#) Alpine Linux Security Update for curl

© [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](#)