



CVE-2018-16840

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

Summary

CVE	CVE-2018-16840
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-31 18:29:00 UTC
Updated	2019-10-09 23:36:00 UTC
Description	A heap use-after-free flaw was found in curl versions from 7.59.0 through 7.61.1 in the code related to closing an easy handle

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Application	Haxx	Curl	All	All	All	All

References

Reference	Source	Link
cURL: Multiple vulnerabilities (GLSA 201903-03) — Gentoo security	GENTOO	security.gentoo.org
curl Use-After-Free Memory Error in Curl_close() Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytracker.com
1642203 – (CVE-2018-16840) CVE-2018-16840 curl: Use-after-free when closing "easy" handle in Curl_close()	CONFIRM	bugzilla.redhat.com
curl - use-after-free in handle close - CVE-2018-16840	MISC	curl.haxx.se
USN-3805-1: curl vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com

Curl_close: clear data->multi_easy on free to avoid use-after-free · curl/curl@81d135d · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [500126](#) Alpine Linux Security Update for curl
- [503781](#) Alpine Linux Security Update for curl
- [710197](#) Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201903-03)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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