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 hanc

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.gent
curl Use-After-Free Memory Error in Curl_close() Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.security
1642203 – (CVE-2018-16840) CVE-2018-16840 curl: Use-after-free when closing "easy" handle in Curl_close()	CONFIRM	bugzilla.redh
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.c

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)