



CVE-2019-3823

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

Summary

CVE	CVE-2019-3823
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-06 20:29:00 UTC
Updated	2023-11-07 03:10:00 UTC
Description	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-re-

Risk And Classification

Problem Types: CWE-125

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
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Haxx	Libcurl	All	All	All	All
Application	Haxx	Libcurl	All	All	All	All
Operating System	Netapp	Clustered Data Ontap	All	All	All	All
Operating System	Netapp	Clustered Data Ontap	All	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All
Application	Oracle	Communications Operations Monitor	4.0	All	All	All
Application	Oracle	Communications Operations Monitor	3.4	All	All	All

Application	Oracle	Communications Operations Monitor	4.0	All	All	All
Application	Oracle	Http Server	12.2.1.3.0	All	All	All
Application	Oracle	Http Server	12.2.1.3.0	All	All	All
Application	Oracle	Secure Global Desktop	5.4	All	All	All
Application	Oracle	Secure Global Desktop	5.4	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4386-1 curl	DEBIAN	www.debian.org	Third Party
cURL: Multiple vulnerabilities (GLSA 201903-03) — Gentoo security	GENTOO	security.gentoo.org	Third Party
cert-portal.siemens.com/productcert/pdf/ssa-936080.pdf	CONFIRM	cert-portal.siemens.com	
curl - SMTP end-of-response out-of-bounds read - CVE-2019-3823	MISC	curl.haxx.se	Patched
February 2019 curl/libcurl Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Exploited
cURL/libcURL Multiple Buffer Overflow Vulnerabilities	BID	www.securityfocus.com	Third Party
USN-3882-1: curl vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Third Party
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
1670256 – (CVE-2019-3823) CVE-2019-3823 curl: SMTP end-of-response out-of-bounds read	CONFIRM	bugzilla.redhat.com	Exploited
Pony Mail!	MLIST	lists.apache.org	Mailing List
Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com	Patched
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296092](#) Oracle Solaris 11.4 Support Repository Update (SRU) 7.1.4 Missing (CPUJAN2019)

[377396](#) Alibaba Cloud Linux Security Update for curl (ALINUX3-SA-2021:0078)

[500127](#) Alpine Linux Security Update for curl

[503782](#) Alpine Linux Security Update for curl

[590673](#) Siemens SCALANCE and SIMATIC libcurl (Update B) Vulnerability (ICSA-21-068-10)

[710197](#) Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201903-03)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)