CVE-2018-1000120

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-1000120
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-14 18:29:00 UTC
Updated	2019-06-18 22:15:00 UTC
Description	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	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	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	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	17.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Haxx	Curl	All	All	All	All
Application	Oracle	Communications Webrtc Session Controller	All	All	All	All
Application	Oracle	Communications Webrtc Session Controller	All	All	All	All

Application	Oracle	Enterprise Manager Ops Center	12.2.2	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.2.2	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.55	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.55	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.redhat.com
curl - FTP path trickery leads to NIL byte out of bounds write - CVE-2018-1000120	CONFIRM	curl.haxx.se
curl FTP Pathname Heap Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.securitytracker.com
Red Hat Customer Portal	REDHAT	access.redhat.com
CPU July 2018	CONFIRM	www.oracle.com
[SECURITY] [DLA 1309-1] curl security update	MLIST	lists.debian.org
Debian -- Security Information -- DSA-4136-1 curl	DEBIAN	www.debian.org
Oracle Critical Patch Update - January 2019	CONFIRM	www.oracle.com
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
USN-3598-2: curl vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
CPU Oct 2018	CONFIRM	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Oracle Critical Patch Update - October 2019	MISC	www.oracle.com
cURL/libcURL CVE-2018-1000120 Buffer Overflow Vulnerability	BID	www.securityfocus.com

USN-3598-1: curl vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.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

500122 Alpine Linux Security Update for curl

503777 Alpine Linux Security Update for curl

710294 Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201804-04)

© 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 registred 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**