



# CVE-2023-23916

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

## Summary

<b>CVE</b>	CVE-2023-23916
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-23 20:15:00 UTC
<b>Updated</b>	2024-03-27 14:54:00 UTC
<b>Description</b>	An allocation of resources without limits or throttling vulnerability exists in curl <v7.88.0 based on the "chained" HTTP comp

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Haxx</a>	<a href="#">Curl</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Clustered Data Ontap</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All
Application	<a href="#">Splunk</a>	<a href="#">Universal Forwarder</a>	All	All	All	All
Application	<a href="#">Splunk</a>	<a href="#">Universal Forwarder</a>	9.1.0	All	All	All

## References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-5365-1 curl	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
[SECURITY] Fedora 36 Update: curl-7.82.0-13.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
HackerOne	MISC	<a href="http://hackerone.com">hackerone.com</a>	
curl: Multiple Vulnerabilities (GLSA 202310-12) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
[SECURITY] Fedora 36 Update: curl-7.82.0-13.fc36 - package-announce - Fedora Mailing-Lists		<a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>	
February 2023 cURL/libcURL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="http://security.netapp.com">security.netapp.com</a>	
[SECURITY] [DLA 3341-1] curl security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canon

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">160501</a> Oracle Enterprise Linux Security Update for curl (ELSA-2023-1140)
<a href="#">160545</a> Oracle Enterprise Linux Security Update for curl (ELSA-2023-1701)
<a href="#">181609</a> Debian Security Update for curl (DLA 3341-1)
<a href="#">181662</a> Debian Security Update for curl (DSA 5365-1)
<a href="#">184640</a> Debian Security Update for curl (CVE-2023-23916)
<a href="#">199191</a> Ubuntu Security Notification for curl Vulnerabilities (USN-5891-1)
<a href="#">241245</a> Red Hat Update for curl (RHSA-2023:1140)
<a href="#">241335</a> Red Hat Update for curl (RHSA-2023:1701)
<a href="#">241356</a> Red Hat Update for curl (RHSA-2023:1842)
<a href="#">241574</a> Red Hat Update for JBoss Core Services (RHSA-2023:3354)
<a href="#">241641</a> Red Hat Update for curl (RHSA-2023:3460)
<a href="#">241829</a> Red Hat Update for curl (RHSA-2023:4139)
<a href="#">283721</a> Fedora Security Update for curl (FEDORA-2023-ddf6575695)
<a href="#">283751</a> Fedora Security Update for curl (FEDORA-2023-94df30cbec)
<a href="#">330140</a> IBM AIX Multiple Vulnerabilities due to curl (curl_advisory2)
<a href="#">354789</a> Amazon Linux Security Advisory for curl : ALAS2-2023-1986
<a href="#">354899</a> Amazon Linux Security Advisory for curl : ALAS-2023-1729

<a href="#">355123</a> Amazon Linux Security Advisory for curl : ALAS2023-2023-114
<a href="#">378120</a> Alibaba Cloud Linux Security Update for curl (ALINUX3-SA-2023:0032)
<a href="#">378438</a> HCL BigFix Multiple Security Vulnerabilities (KB0103724)
<a href="#">378453</a> NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Denial of Service (DoS) Vulnerability (NTAP-20230309-0006)
<a href="#">378560</a> IBM MQ LibcURL Multiple Vulnerabilities (6952185)
<a href="#">378599</a> Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)
<a href="#">378883</a> Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
<a href="#">502664</a> Alpine Linux Security Update for curl
<a href="#">502667</a> Alpine Linux Security Update for curl
<a href="#">502668</a> Alpine Linux Security Update for curl
<a href="#">502719</a> Alpine Linux Security Update for curl
<a href="#">503103</a> Alpine Linux Security Update for curl
<a href="#">505861</a> Alpine Linux Security Update for curl
<a href="#">672874</a> EulerOS Security Update for curl (EulerOS-SA-2023-1590)
<a href="#">672973</a> EulerOS Security Update for curl (EulerOS-SA-2023-1838)
<a href="#">672997</a> EulerOS Security Update for curl (EulerOS-SA-2023-1862)
<a href="#">673128</a> EulerOS Security Update for curl (EulerOS-SA-2023-2286)
<a href="#">673152</a> EulerOS Security Update for curl (EulerOS-SA-2023-2262)
<a href="#">691083</a> Free Berkeley Software Distribution (FreeBSD) Security Update for curl (be233fc6-bae7-11ed-a4fb-080027f5fec9)
<a href="#">710772</a> Gentoo Linux curl Multiple Vulnerabilities (GLSA 202310-12)
<a href="#">753701</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:0425-1)
<a href="#">753702</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:0429-1)
<a href="#">753857</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:1711-1)
<a href="#">754020</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:2226-1)
<a href="#">754021</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:2228-1)
<a href="#">905583</a> Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (13632)
<a href="#">905587</a> Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13628)
<a href="#">905588</a> Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13636)

905589 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (13627)
905594 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (13657)
905595 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13653)
905597 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13658)
905601 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (13651)
906619 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13653-3)
906699 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13628-1)
906873 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (13657-1)
907408 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13658-1)
940957 AlmaLinux Security Update for curl (ALSA-2023:1140)
940984 AlmaLinux Security Update for curl (ALSA-2023:1701)
960671 Rocky Linux Security Update for curl (RLSA-2023:1140)

© [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](#)**