



# CVE-2021-22925

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

## Summary

<b>CVE</b>	CVE-2021-22925
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-05 21:15:00 UTC
<b>Updated</b>	2024-03-27 15:11:00 UTC
<b>Description</b>	curl supports the <code>-t</code> command line option, known as <code>CURLLOPT_TELNETOPTIONS</code> in libcurl. This rarely used option is us

## Risk And Classification

**Problem Types:** CWE-908

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.0	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.0.1	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.1	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.1.0	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.2	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.2.1	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.3	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.3.1	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.4	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	11.5	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	-	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-002	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-003	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-004	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Haxx</a>	<a href="#">Curl</a>	All	All	All	All

Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Oracle	Mysql Server	All	All	All	All
Application	Oracle	Mysql Server	All	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.59	All	All	All
Application	Siemens	Sinec Infrastructure Network Services	All	All	All	All
Application	Siemens	Sinema Remote Connect Server	All	All	All	All
Application	Splunk	Universal Forwarder	All	All	All	All
Application	Splunk	Universal Forwarder	9.1.0	All	All	All

## References

Reference	Source
Full Disclosure: APPLE-SA-2021-09-20-7 Additional information for APPLE-SA-2021-09-13-3 macOS Big Sur 11.6	FULLDISC
August 2021 cURL/libcURL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM
curl: Multiple Vulnerabilities (GLSA 202212-01) — Gentoo security	GENTOO
About the security content of Security Update 2021-005 Catalina - Apple Support	CONFIRM
About the security content of macOS Big Sur 11.6 - Apple Support	CONFIRM

Full Disclosure: APPLE-SA-2021-09-20-8 Additional information for APPLE-SA-2021-09-13-4 Security Update 2021-005 Catalina	FULLDISC
Oracle Critical Patch Update Advisory - October 2021	MISC
HackerOne	MISC
Oracle Critical Patch Update Advisory - January 2022	MISC
cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf	CONFIRM
[SECURITY] Fedora 33 Update: curl-7.71.1-10.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
[SECURITY] Fedora 33 Update: curl-7.71.1-10.fc33 - package-announce - Fedora Mailing-Lists	FEDORA
cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">159520</a> Oracle Enterprise Linux Security Update for curl (ELSA-2021-4511)
<a href="#">198441</a> Ubuntu Security Notification for curl vulnerabilities (USN-5021-1)
<a href="#">199491</a> Ubuntu Security Notification for curl Vulnerabilities (USN-5894-1)
<a href="#">239832</a> Red Hat Update for curl (RHSA-2021:4511)
<a href="#">281737</a> Fedora Security Update for curl (FEDORA-2021-83fdddca0f)
<a href="#">281795</a> Fedora Security Update for curl (FEDORA-2021-5d21b90a30)
<a href="#">296065</a> Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)
<a href="#">352843</a> Amazon Linux Security Advisory for curl: ALAS2-2021-1700
<a href="#">376257</a> Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUJAN2022)
<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="#">500136</a> Alpine Linux Security Update for curl
<a href="#">503787</a> Alpine Linux Security Update for curl
<a href="#">591406</a> Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
<a href="#">670699</a> EulerOS Security Update for curl (EulerOS-SA-2021-2457)
<a href="#">670824</a> EulerOS Security Update for curl (EulerOS-SA-2021-2707)
<a href="#">670975</a> EulerOS Security Update for curl (EulerOS-SA-2021-2656)
<a href="#">671008</a> EulerOS Security Update for curl (EulerOS-SA-2021-2682)

<a href="#">071006</a> EulerOS Security Update for curl (EulerOS-SA-2021-2062)
<a href="#">671718</a> EulerOS Security Update for curl (EulerOS-SA-2022-1711)
<a href="#">690083</a> Free Berkeley Software Distribution (FreeBSD) Security Update for curl (aa646c01-ea0d-11eb-9b84-d4c9ef517024)
<a href="#">710693</a> Gentoo Linux curl Multiple Vulnerabilities (GLSA 202212-01)
<a href="#">750866</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2021:2425-1)
<a href="#">750872</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2021:2440-1)
<a href="#">750875</a> OpenSUSE Security Update for curl (openSUSE-SU-2021:2439-1)
<a href="#">750888</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2021:2462-1)
<a href="#">750891</a> OpenSUSE Security Update for curl (openSUSE-SU-2021:1088-1)
<a href="#">900298</a> CBL-Mariner Linux Security Update for curl 7.76.0
<a href="#">900909</a> Common Base Linux Mariner (CBL-Mariner) Security Update for curl (6363-1)
<a href="#">903395</a> Common Base Linux Mariner (CBL-Mariner) Security Update for curl (5210)
<a href="#">940095</a> AlmaLinux Security Update for curl (ALSA-2021:4511)
<a href="#">960010</a> Rocky Linux Security Update for curl (RLSA-2021:4511)

© [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](#)**