



# CVE-2020-8286

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

## Summary

<b>CVE</b>	CVE-2020-8286
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-14 20:15:00 UTC
<b>Updated</b>	2024-03-27 15:47:00 UTC
<b>Description</b>	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the C

## Risk And Classification

**Problem Types:** CWE-295

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	-	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2019-001	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2019-002	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-001	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-002	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-003	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-004	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-005	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-006	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2020-007	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.14.6	security_update_2021-001	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	-	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2020-001	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-001	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	supplemental_update	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All
Application	<a href="#">Haxx</a>	<a href="#">Libcurl</a>	All	All	All
Application	<a href="#">Haxx</a>	<a href="#">Libcurl</a>	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Clusted Data Ontap</a>	-	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Hci Bootstrap Os</a>	-	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Compute Node</a>	-	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Storage Node</a>	-	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Hci Storage Node Firmware</a>	-	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Billing And Revenue Management</a>	12.0.0.3.0	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Cloud Native Core Policy</a>	1.14.0	All	All
Application	<a href="#">Oracle</a>	<a href="#">Essbase</a>	21.2	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.58	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Simatic Tim 1531 Irc</a>	-	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Simatic Tim 1531 Irc Firmware</a>	All	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Infrastructure Network Services</a>	All	All	All
Application	<a href="#">Splunk</a>	<a href="#">Universal Forwarder</a>	All	All	All
Application	<a href="#">Splunk</a>	<a href="#">Universal Forwarder</a>	9.1.0	All	All

## References

Reference	Source	Link	Tags
<a href="#">curl - Inferior OCSP verification - CVE-2020-8286</a>	MISC	<a href="#">curl.se</a>	Vulnerability
<a href="#">cURL: Multiple vulnerabilities (GLSA 202012-14) — Gentoo security</a>	GENTOO	<a href="#">security.gentoo.org</a>	
<a href="#">Debian -- Security Information -- DSA-4881-1 curl</a>	DEBIAN	<a href="#">www.debian.org</a>	
<a href="#">Oracle Critical Patch Update Advisory - April 2022</a>	MISC	<a href="#">www.oracle.com</a>	
<a href="#">[SECURITY] [DLA 2500-1] curl security update</a>	MLIST	<a href="#">lists.debian.org</a>	Mailing List
<a href="#">Oracle Critical Patch Update Advisory - July 2021</a>	N/A	<a href="#">www.oracle.com</a>	
<a href="#">[SECURITY] Fedora 32 Update: curl-7.69.1-7.fc32 - package-announce - Fedora Mailing-Lists</a>		<a href="#">lists.fedoraproject.org</a>	

[SECURITY] Fedora 32 Update: curl-7.69.1-7.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third
Full Disclosure: APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
About the security content of Security Update 2021-002 Catalina - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>	
About the security content of Security Update 2021-003 Mojave - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>	
December 2020 cURL/libcURL Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf">cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
[SECURITY] Fedora 33 Update: curl-7.71.1-8.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 33 Update: curl-7.71.1-8.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Third
HackerOne	MISC	<a href="https://hackerone.com">hackerone.com</a>	Expl
About the security content of macOS Big Sur 11.3 - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>	
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>	
Full Disclosure: APPLE-SA-2021-04-26-4 Security Update 2021-003 Mojave	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-200951.pdf">cert-portal.siemens.com/productcert/pdf/ssa-200951.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
Full Disclosure: APPLE-SA-2021-04-26-2 macOS Big Sur 11.3	FULLDISC	<a href="https://seclists.org">seclists.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canc

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [12304](#) McAfee Web Gateway Product Multiple Vulnerabilities (WP-2326,WP-3443)
- [159196](#) Oracle Enterprise Linux Security Update for curl (ELSA-2021-1610)
- [178522](#) Debian Security Update for curl (DSA 4881-1)
- [239328](#) Red Hat Update for curl (RHSA-2021:1610)
- [239451](#) Red Hat Update for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 SP8 (RHSA-2021:2472)
- [296067](#) Oracle Solaris 11.4 Support Repository Update (SRU) 33.94.0 Missing (CPUAPR2021)
- [352506](#) Amazon Linux Security Advisory for curl: ALAS2-2021-1693
- [375482](#) Oracle PeopleSoft Enterprise PeopleTools Product Multiple Vulnerabilities (CPUAPR2021)
- [375503](#) Apple macOS Big Sur 11.3 Not Installed (HT212325)
- [375507](#) Apple macOS Security Update 2021-002 Catalina (HT212326)
- [375510](#) Apple macOS Security Update 2021-003 Mojave (HT212327)
- [376969](#) NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information Vulnerability (NTAP-20210122-0007)

377396 Alibaba Cloud Linux Security Update for curl (ALINUX3-SA-2021:0078)
378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)
378883 Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)
44183 Juniper Network Operating System (Junos OS) Multiple Security Vulnerabilities (JSA79108)
500132 Alpine Linux Security Update for curl
501396 Alpine Linux Security Update for curl
503888 Alpine Linux Security Update for curl
590737 Siemens SIMATIC TIM libcurl Multiple Vulnerabilities (ICSA-21-159-10)
590738 Siemens Industrial Products LLDP Multiple Vulnerabilities (ICSA-21-194-07)
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
690348 Free Berkeley Software Distribution (FreeBSD) Security Update for curl (3c77f139-3a09-11eb-929d-d4c9ef517024)
750055 SUSE Enterprise Linux Security Update for curl (SUSE-SU-2021:1786-1)
750490 OpenSUSE Security Update for curl (openSUSE-SU-2020:2249-1)
750492 OpenSUSE Security Update for curl (openSUSE-SU-2020:2238-1)
900155 CBL-Mariner Linux Security Update for curl 7.68.0
902979 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (3666)
940000 AlmaLinux Security Update for curl (ALSA-2021:1610)
960740 Rocky Linux Security Update for curl (RLSA-2021:1610)

© [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](#)**