



CVE-2020-8285

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

Summary

CVE	CVE-2020-8285
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-14 20:15:00 UTC
Updated	2024-03-27 15:47:00 UTC
Description	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard mat

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition
Operating System	Apple	Macos	All	All	All
Operating System	Apple	Mac Os X	All	All	All
Operating System	Apple	Mac Os X	10.14.6	-	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-001	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-002	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-001	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-002	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-003	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-004	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-005	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-006	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-007	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2021-001	All
Operating System	Apple	Mac Os X	10.15.7	-	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2020-001	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-001	All
Operating System	Apple	Mac Os X	10.15.7	supplemental_update	All

Operating System	Debian	Debian Linux	10.0	All	All
Operating System	Debian	Debian Linux	9.0	All	All
Operating System	Debian	Debian Linux	9.0	All	All
Operating System	Fedoraproject	Fedora	32	All	All
Operating System	Fedoraproject	Fedora	33	All	All
Operating System	Fedoraproject	Fedora	32	All	All
Operating System	Fedoraproject	Fedora	33	All	All
Hardware	Fujitsu	M10-1	-	All	All
Operating System	Fujitsu	M10-1 Firmware	All	All	All
Hardware	Fujitsu	M10-4	-	All	All
Hardware	Fujitsu	M10-4s	-	All	All
Operating System	Fujitsu	M10-4s Firmware	All	All	All
Operating System	Fujitsu	M10-4 Firmware	All	All	All
Hardware	Fujitsu	M12-1	-	All	All
Operating System	Fujitsu	M12-1 Firmware	All	All	All
Hardware	Fujitsu	M12-2	-	All	All
Hardware	Fujitsu	M12-2s	-	All	All
Operating System	Fujitsu	M12-2s Firmware	All	All	All
Operating System	Fujitsu	M12-2 Firmware	All	All	All
Application	Haxx	Libcurl	All	All	All
Application	Haxx	Libcurl	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All
Operating System	Netapp	Hci Bootstrap Os	-	All	All
Hardware	Netapp	Hci Compute Node	-	All	All
Application	Netapp	Hci Management Node	-	All	All
Hardware	Netapp	Hci Storage Node	-	All	All
Operating System	Netapp	Hci Storage Node Firmware	-	All	All
Application	Netapp	Solidfire	-	All	All
Application	Oracle	Communications Billing And Revenue Management	12.0.0.3.0	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.14.0	All	All
Application	Oracle	Essbase	21.2	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All	All
Application	Siemens	Sinec Infrastructure Network Services	All	All	All
Application	Splunk	Universal Forwarder	All	All	All
Application	Splunk	Universal Forwarder	9.1.0	All	All

References

Reference

[cURL: Multiple vulnerabilities \(GLSA 202012-14\) — Gentoo security](#)

[Debian -- Security Information -- DSA-4881-1 curl](#)

[\[bookkeeper-issues\] 20210628 \[GitHub\] \[bookkeeper\] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade](#)

[Oracle Critical Patch Update Advisory - April 2022](#)

[Pony Mail!](#)

[\[SECURITY\] \[DLA 2500-1\] curl security update](#)

[HackerOne](#)

[Oracle Critical Patch Update Advisory - July 2021](#)

[\[SECURITY\] Fedora 32 Update: curl-7.69.1-7.fc32 - package-announce - Fedora Mailing-Lists](#)

[Oracle Critical Patch Update Advisory - January 2022](#)

[\[SECURITY\] Fedora 32 Update: curl-7.69.1-7.fc32 - package-announce - Fedora Mailing-Lists](#)

[Full Disclosure: APPLE-SA-2021-04-26-3 Security Update 2021-002 Catalina](#)

[About the security content of Security Update 2021-002 Catalina - Apple Support](#)

[About the security content of Security Update 2021-003 Mojave - Apple Support](#)

[December 2020 cURL/libcURL Vulnerabilities in NetApp Products | NetApp Product Security](#)

[cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf](#)

[\[SECURITY\] Fedora 33 Update: curl-7.71.1-8.fc33 - package-announce - Fedora Mailing-Lists](#)

[Pony Mail!](#)

[\[bookkeeper-issues\] 20210629 \[GitHub\] \[bookkeeper\] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade](#)

[\[SECURITY\] Fedora 33 Update: curl-7.71.1-8.fc33 - package-announce - Fedora Mailing-Lists](#)

[curl - FTP wildcard stack overflow - CVE-2020-8285](#)

[About the security content of macOS Big Sur 11.3 - Apple Support](#)

[Stack overflow in libcurl when CURLOPT_WILDCARDMATCH is in use · Issue #6255 · curl/curl · GitHub](#)

[Oracle Critical Patch Update Advisory - April 2021](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

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
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)
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
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
670172 EulerOS Security Update for curl (EulerOS-SA-2021-1672)
670912 EulerOS Security Update for curl (EulerOS-SA-2021-1287)
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
903147 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (3665)
940000 AlmaLinux Security Update for curl (ALSA-2021:1610)
960740 Rocky Linux Security Update for curl (RLSA-2021:1610)

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](#)