CVE-2020-8284

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8284
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 15:50:00 UTC
Description	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP addre

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition
Operating System	Apple	Macos	11.0.1	All	All
Operating System	Apple	Macos	11.1	All	All
Operating System	Apple	Macos	11.2	All	All
Operating System	Apple	Mac Os X	All	All	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_2019-004	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-005	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-006	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-007	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	10.14.6	security_update_2021-002	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update_2	All
Operating System	Apple	Mac Os X	10.15.7	-	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2020	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_2020-005	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2020-007	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	Curl	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
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	Source	Link	Tags
cURL: Multiple vulnerabilities (GLSA 202012-14) — Gentoo security	GENTOO	security.gentoo.org	
Debian -- Security Information -- DSA-4881-1 curl	DEBIAN	www.debian.org	
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
[SECURITY] [DLA 2500-1] curl security update	MLIST	lists.debian.org	Maili
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
[SECURITY] Fedora 32 Update: curl-7.69.1-7.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com	
[SECURITY] Fedora 32 Update: curl-7.69.1-7.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third
About the security content of Security Update 2021-002 Catalina - Apple Support	CONFIRM	support.apple.com	
About the security content of Security Update 2021-003 Mojave - Apple Support	CONFIRM	support.apple.com	
December 2020 cURL/libcURL Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf	CONFIRM	cert-portal.siemens.com	
[SECURITY] Fedora 33 Update: curl-7.71.1-8.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: curl-7.71.1-8.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third
About the security content of macOS Big Sur 11.3 - Apple Support	CONFIRM	support.apple.com	
HackerOne	MISC	hackerone.com	Perm
curl - trusting FTP PASV responses - CVE-2020-8284	MISC	curl.se	Vend
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159196 Oracle Enterprise Linux Security Update for curl (ELSA-2021-1610)

178522 Debian Security Update for curl (DSA 4881-1)

181247 Debian Security Update for inetutils (DLA 3205-1)

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

376053 F5 BIG-IP Local Traffic Manager (LTM), Access Policy Manager (APM), Application Security Manager (ASM) cURL Vulnerability (K63525058)

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 Vulnerabilites (JSA79108)

500133 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)

670356 EulerOS Security Update for curl (EulerOS-SA-2021-1868)

670383 EulerOS Security Update for curl (EulerOS-SA-2021-1942)

670404 EulerOS Security Update for curl (EulerOS-SA-2021-1921)

671343 EulerOS Security Update for curl (EulerOS-SA-2022-1265)

671718 EulerOS Security Update for curl (EulerOS-SA-2022-1711)

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

903483 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (3675)

940000 AlmaLinux Security Update for curl (ALSA-2021:1610)

960740 Rocky Linux Security Update for curl (RLSA-2021:1610)