



# CVE-2023-27534

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-27534
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-30 20:15:00 UTC
<b>Updated</b>	2024-03-27 14:54:00 UTC
<b>Description</b>	A path traversal vulnerability exists in curl <8.0.0 SFTP implementation causes the tilde (~) character to be wrongly replace

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Broadcom</a>	<a href="#">Brocade Fabric Operating System Firmware</a>	-	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="#">Active Iq Unified Manager</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-lts-announce] 20240317 [SECURITY] [DLA 3763-1] curl security update			<a href="https://lists.debian.org">lists.debian.org</a>
curl: Multiple Vulnerabilities (GLSA 202310-12) — Gentoo security	GENTOO		<a href="https://security.gentoo.org">security.gentoo.org</a>
CVE-2023-27534 cURL/libcURL Vulnerability in NetApp Products   NetApp Product Security	CONFIRM		<a href="https://security.netapp.com">security.netapp.com</a>
HackerOne	MISC		<a href="https://hackerone.com">hackerone.com</a>
[SECURITY] Fedora 36 Update: curl-7.82.0-14.fc36 - package-announce - Fedora Mailing-Lists			<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 36 Update: curl-7.82.0-14.fc36 - package-announce - Fedora Mailing-Lists	FEDORA		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canon

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[161067](#) Oracle Enterprise Linux Security Update for curl (ELSA-2023-6679)

[182456](#) Debian Security Update for curl (CVE-2023-27534)

[199246](#) Ubuntu Security Notification for curl Vulnerabilities (USN-5964-1)

[242295](#) Red Hat Update for curl (RHSA-2023:6679)

[283820](#) Fedora Security Update for curl (FEDORA-2023-2884ba1528)

[283865](#) Fedora Security Update for curl (FEDORA-2023-7e7414e64d)

[284222](#) Fedora Security Update for curl (FEDORA-2023-0de03a9232)

[330140](#) IBM AIX Multiple Vulnerabilities due to curl (curl\_advisory2)

[354899](#) Amazon Linux Security Advisory for curl : ALAS-2023-1729

[355077](#) Amazon Linux Security Advisory for curl : AL2012-2023-401

[355390](#) Amazon Linux Security Advisory for curl : ALAS2-2023-2070

[355415](#) Amazon Linux Security Advisory for curl : ALAS2023-2023-193

[378599](#) Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

[378883](#) Splunk Enterprise August Third Party Package Updates (SVD-2023-0808)

[502707](#) Alpine Linux Security Update for curl

[502720](#) Alpine Linux Security Update for curl

[503104](#) Alpine Linux Security Update for curl

[505862](#) Alpine Linux Security Update for curl

[6000526](#) Debian Security Update for curl (DLA 3763-1)

672889 EulerOS Security Update for curl (EulerOS-SA-2023-1816)
672907 EulerOS Security Update for curl (EulerOS-SA-2023-1798)
673091 EulerOS Security Update for curl (EulerOS-SA-2023-2188)
673174 EulerOS Security Update for curl (EulerOS-SA-2023-2308)
673187 EulerOS Security Update for curl (EulerOS-SA-2023-2328)
673616 EulerOS Security Update for curl (EulerOS-SA-2023-2635)
673678 EulerOS Security Update for curl (EulerOS-SA-2023-2677)
691088 Free Berkeley Software Distribution (FreeBSD) Security Update for curl (0d7d104c-c6fb-11ed-8a4b-080027f5fec9)
710772 Gentoo Linux curl Multiple Vulnerabilities (GLSA 202310-12)
753819 SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:0865-1)
753857 SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:1711-1)
754020 SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:2226-1)
754021 SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:2228-1)
906750 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (25847-1)
907401 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (25810-1)
907640 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (25806-1)
941357 AlmaLinux Security Update for curl (ALSA-2023:6679)

© [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](#)**