



# CVE-2023-38545

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

## Summary

<b>CVE</b>	CVE-2023-38545
<b>State</b>	PUBLIC
<b>Assigner</b>	support@hackerone.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-10-18 04:15:00 UTC
<b>Updated</b>	2024-04-01 15:45:00 UTC
<b>Description</b>	This flaw makes curl overflow a heap based buffer in the SOCKS5 proxy handshake. When curl is asked to pass along the

## Risk And Classification

**Problem Types: CWE-787**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Haxx</a>	<a href="#">Libcurl</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10 1809</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10 21h2</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 10 22h2</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 11 21h2</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 11 22h2</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows 11 23h2</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Server 2019</a>	All	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Server 2022</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Insight</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Workflow Automation</a>	-	All	All	All

## References

Reference	Source	Link	Tags
-----------	--------	------	------

January 2024 MySQL Cluster Vulnerabilities in NetApp Products   NetApp Product Security		<a href="https://security.netapp.com">security.netapp.com</a>	
[SECURITY] Fedora 37 Update: curl-7.85.0-12.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
curl - SOCKS5 heap buffer overflow - CVE-2023-38545	MISC	<a href="https://curl.se">curl.se</a>	
About the security content of macOS Ventura 13.6.4 - Apple Support		<a href="https://support.apple.com">support.apple.com</a>	
About the security content of macOS Sonoma 14.2 - Apple Support		<a href="https://support.apple.com">support.apple.com</a>	
<a href="https://www.secpod.com/blog/high-severity-heap-buffer-overflow-vulnerability">www.secpod.com/blog/high-severity-heap-buffer-overflow-vulnerability</a>		<a href="https://www.secpod.com">www.secpod.com</a>	
<a href="https://seclists.org/fulldisclosure/2024/Jan/37">seclists.org/fulldisclosure/2024/Jan/37</a>		<a href="https://seclists.org">seclists.org</a>	
October 2023 MySQL Server Vulnerabilities in NetApp Products   NetApp Product Security	MISC	<a href="https://security.netapp.com">security.netapp.com</a>	
<a href="https://seclists.org/fulldisclosure/2024/Jan/38">seclists.org/fulldisclosure/2024/Jan/38</a>		<a href="https://seclists.org">seclists.org</a>	
<a href="https://seclists.org/fulldisclosure/2024/Jan/34">seclists.org/fulldisclosure/2024/Jan/34</a>		<a href="https://seclists.org">seclists.org</a>	
About the security content of macOS Monterey 12.7.3 - Apple Support		<a href="https://support.apple.com">support.apple.com</a>	
About the security content of iOS 16.7.5 and iPadOS 16.7.5 - Apple Support		<a href="https://support.apple.com">support.apple.com</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

- [160994](#) Oracle Enterprise Linux Security Update for curl (ELSA-2023-5763)
- [161081](#) Oracle Enterprise Linux Security Update for curl (ELSA-2023-6745)
- [199825](#) Ubuntu Security Notification for curl Vulnerabilities (USN-6429-1)
- [199899](#) Ubuntu Security Notification for curl Vulnerabilities (USN-6429-3)
- [20369](#) Oracle MySQL OCT 2023 Critical Patch Update (CPUOCT2023)
- [20399](#) Oracle Database 19c Critical OJVM Patch Update - January 2024
- [20400](#) Oracle Database 19c Critical Patch Update - January 2024
- [20401](#) Oracle Database 21c Critical Patch Update - January 2024
- [242165](#) Red Hat Update for curl (RHSA-2023:5700)
- [242183](#) Red Hat Update for curl (RHSA-2023:5763)
- [242283](#) Red Hat Update for curl (RHSA-2023:6745)
- [242553](#) Red Hat Update for JBoss Core Services (RHSA-2023:7625)
- [242923](#) Red Hat Update for Satellite 6.14.2 (RHSA-2024:0797)
- [284621](#) Fedora Security Update for curl (FEDORA-2023-b855de5c0f)

<a href="#">284684</a> Fedora Security Update for curl (FEDORA-2023-fef2b8da32)
<a href="#">285202</a> Fedora Security Update for curl (FEDORA-2023-0f8d1871d8)
<a href="#">296105</a> Oracle Solaris 11.4 Support Repository Update (SRU) 63.157.1 Missing (CPUOCT2023)
<a href="#">296106</a> Oracle Solaris 11.4 Support Repository Update (SRU) 64.157.2 Missing (CPUOCT2023)
<a href="#">330154</a> IBM AIX Multiple Vulnerabilities due to curl (curl_advisory3)
<a href="#">356311</a> Amazon Linux Security Advisory for curl : ALAS2023-2023-377
<a href="#">356312</a> Amazon Linux Security Advisory for curl : ALAS2-2023-2287
<a href="#">378936</a> Microsoft Windows Curl Multiple Security Vulnerabilities
<a href="#">378999</a> Curl Heap Buffer Overflow Vulnerability
<a href="#">379000</a> Curl SOCKS5 Heap Buffer Overflow Vulnerability
<a href="#">379002</a> Libcurl Heap Buffer Overflow Vulnerability
<a href="#">379266</a> Oracle Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (CPUJAN2024)
<a href="#">379298</a> Apple macOS Ventura 13.6.4 Not Installed (HT214058)
<a href="#">379300</a> Apple macOS Monterey 12.7.3 Not Installed (HT214057)
<a href="#">379346</a> HCL BigFix Multiple Security Vulnerabilities (KB0110209)
<a href="#">379590</a> Gitlab Multiple Vulnerabilities (prior to gitlab- 16.5.1, 16.4.2, 16.3.6)
<a href="#">44136</a> FortiOS Multiple Vulnerabilities (FG-IR-23-385)
<a href="#">44183</a> Juniper Network Operating System (Junos OS) Multiple Security Vulnerabilites (JSA79108)
<a href="#">503379</a> Alpine Linux Security Update for curl
<a href="#">505864</a> Alpine Linux Security Update for curl
<a href="#">6000245</a> Debian Security Update for curl (DSA 5523-1)
<a href="#">610539</a> Apple iOS 16.7.5 and iPadOS 16.7.5 Security Update Missing (HT214063)
<a href="#">673709</a> EulerOS Security Update for curl (EulerOS-SA-2023-3239)
<a href="#">673772</a> EulerOS Security Update for curl (EulerOS-SA-2024-1055)
<a href="#">673815</a> EulerOS Security Update for curl (EulerOS-SA-2023-3294)
<a href="#">673909</a> EulerOS Security Update for curl (EulerOS-SA-2024-1079)
<a href="#">673989</a> EulerOS Security Update for curl (EulerOS-SA-2023-3267)
<a href="#">674037</a> EulerOS Security Update for curl (EulerOS-SA-2023-3326)
<a href="#">681600</a> EulerOS Security Update for curl (EulerOS-SA-2023-3326)

<a href="#">691322</a> Free Berkeley Software Distribution (FreeBSD) Security Update for curl (d6c19e8c-6806-11ee-9464-b42e9911c52e)
<a href="#">691336</a> Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (22df5074-71cd-11ee-85eb-84a93843eb75)
<a href="#">710772</a> Gentoo Linux curl Multiple Vulnerabilities (GLSA 202310-12)
<a href="#">755070</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:4044-1)
<a href="#">755071</a> SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:4043-1)
<a href="#">907390</a> Common Base Linux Mariner (CBL-Mariner) Security Update for curl (31288-1)
<a href="#">907455</a> Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (31501)
<a href="#">907481</a> Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (31501-1)
<a href="#">941303</a> AlmaLinux Security Update for curl (ALSA-2023:5763)
<a href="#">941348</a> AlmaLinux Security Update for curl (ALSA-2023:6745)
<a href="#">961057</a> Rocky Linux Security Update for curl (RLSA-2023:5763)

© [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](#)**