



CVE-2023-23915

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

Summary

CVE	CVE-2023-23915
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-23 20:15:00 UTC
Updated	2024-03-27 14:55:00 UTC
Description	A cleartext transmission of sensitive information vulnerability exists in curl <v7.88.0 that could cause HSTS functionality to k

Risk And Classification

Problem Types: CWE-319

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haxx	Curl	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Clustered Data Ontap	9.0	-	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Splunk	Universal Forwarder	All	All	All	All
Application	Splunk	Universal Forwarder	9.1.0	All	All	All

References

Reference	Source	Link	Tags
HackerOne	MISC	hackerone.com	Exploit, Issu

HackerOne	MISC	hackerone.com	
curl: Multiple Vulnerabilities (GLSA 202310-12) — Gentoo security	GENTOO	security.gentoo.org	
February 2023 cURL/libcURL Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

183568 Debian Security Update for curl (CVE-2023-23915)
199191 Ubuntu Security Notification for curl Vulnerabilities (USN-5891-1)
241574 Red Hat Update for JBoss Core Services (RHSA-2023:3354)
283721 Fedora Security Update for curl (FEDORA-2023-ddf6575695)
354789 Amazon Linux Security Advisory for curl : ALAS2-2023-1986
355123 Amazon Linux Security Advisory for curl : ALAS2023-2023-114
378453 NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Denial of Service (DoS) Vulnerability (NTAP-20230309-0006)
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)
502664 Alpine Linux Security Update for curl
502667 Alpine Linux Security Update for curl
502668 Alpine Linux Security Update for curl
502719 Alpine Linux Security Update for curl
503103 Alpine Linux Security Update for curl
505861 Alpine Linux Security Update for curl
673128 EulerOS Security Update for curl (EulerOS-SA-2023-2286)
673152 EulerOS Security Update for curl (EulerOS-SA-2023-2262)
691083 Free Berkeley Software Distribution (FreeBSD) Security Update for curl (be233fc6-bae7-11ed-a4fb-080027f5fec9)
710772 Gentoo Linux curl Multiple Vulnerabilities (GLSA 202310-12)
753702 SUSE Enterprise Linux Security Update for curl (SUSE-SU-2023:0429-1)

905585 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13629)
905586 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13634)
905590 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (13626)
905591 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (13631)
905593 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13660)
905596 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (13649)
905600 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (13655)
905603 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13652)
906639 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13652-3)
906700 Common Base Linux Mariner (CBL-Mariner) Security Update for curl (13629-1)
906854 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (13655-1)
907421 Common Base Linux Mariner (CBL-Mariner) Security Update for rust (13660-1)

© [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](#)