



CVE-2023-35945

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

Summary

CVE	CVE-2023-35945
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-13 21:15:00 UTC
Updated	2023-10-24 17:26:00 UTC
Description	Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy's HTTP/2 codec may leak a header map and b

Risk And Classification

Problem Types: CWE-459

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Envoyproxy	Envoy	All	All	All	All
Application	Nghttp2	Nghttp2	All	All	All	All

References

Reference	Source	Link	Tags
github.com/nghttp2/nghttp2/blob/e7f59406556c80904b81b593d38508591bb7523a...	MISC	github.com	
HTTP/2 memory leak in nghttp2 codec · Advisory · envoyproxy/envoy · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[355759](#) Amazon Linux Security Advisory for nghttp2 : ALAS-2023-1793

[355779](#) Amazon Linux Security Advisory for nghttp2 : ALAS2-2023-2180

[355802](#) Amazon Linux Security Advisory for nodejs : ALAS2023-2023-290

[355811](#) Amazon Linux Security Advisory for nghttp2 : ALAS2023-2023-278

355870	Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2023-2023-300
503044	Alpine Linux Security Update for nhttp2
503048	Alpine Linux Security Update for nhttp2
503051	Alpine Linux Security Update for nhttp2
673636	EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3346)
673794	EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3224)
673870	EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3038)
673906	EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3189)
673934	EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3015)
674095	EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3314)
754949	SUSE Enterprise Linux Security Update for nhttp2 (SUSE-SU-2023:3842-1)
755049	SUSE Enterprise Linux Security Update for nhttp2 (SUSE-SU-2023:3997-1)
755101	SUSE Enterprise Linux Security Update for nhttp2 (SUSE-SU-2023:4102-1)
907095	Common Base Linux Mariner (CBL-Mariner) Security Update for nhttp2 (27682-1)
907279	Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (27667-1)
907304	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs18 (27683-1)
907330	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (27650-1)

© [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](#)