



CVE-2023-32067

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-32067
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-25 23:15:00 UTC
Updated	2023-10-31 16:06:00 UTC
Description	c-ares is an asynchronous resolver library. c-ares is vulnerable to denial of service. If a target resolver sends a query, the a

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C-ares Project	C-ares	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All

References

Reference	Source	Link	Tags
0-byte UDP payload Denial of Service · Advisory · c-ares/c-ares · GitHub	MISC	github.com	
[SECURITY] Fedora 38 Update: c-ares-1.19.1-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org	
Release 1.19.1 · c-ares/c-ares · GitHub	MISC	github.com	
[SECURITY] [DLA 3471-1] c-ares security update	MISC	lists.debian.org	
c-ares: Multiple Vulnerabilities (GLSA 202310-09) — Gentoo security	MISC	security.gentoo.org	
Debian -- Security Information -- DSA-5419-1 c-ares	MISC	www.debian.org	
[SECURITY] Fedora 37 Update: c-ares-1.19.1-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org	
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

[160727](#) Oracle Enterprise Linux Security Update for c-ares (ELSA-2023-3559)

[160732](#) Oracle Enterprise Linux Security Update for nodejs (ELSA-2023-3586)

[160734](#) Oracle Enterprise Linux Security Update for c-ares (ELSA-2023-3584)

[160740](#) Oracle Enterprise Linux Security Update for 18 (ELSA-2023-3577)

[160749](#) Oracle Enterprise Linux Security Update for c-ares (ELSA-2023-3741)

[160788](#) Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2023-4034)

[160794](#) Oracle Enterprise Linux Security Update for nodejs:18 (ELSA-2023-4035)

[181829](#) Debian Security Update for c-ares (DSA 5419-1)

[183112](#) Debian Security Update for c-ares (CVE-2023-32067)

[199418](#) Ubuntu Security Notification for c-ares Vulnerabilities (USN-6164-1)

[241698](#) Red Hat Update for c-ares (RHSA-2023:3559)

[241702](#) Red Hat Update for nodejs:18 (RHSA-2023:3577)

[241710](#) Red Hat Update for c-ares (RHSA-2023:3584)

[241717](#) Red Hat Update for c-ares (RHSA-2023:3583)

[241724](#) Red Hat Update for nodejs (RHSA-2023:3586)

[241728](#) Red Hat Update for c-ares (RHSA-2023:3665)

[241729](#) Red Hat Update for c-ares (RHSA-2023:3660)

[241730](#) Red Hat Update for c-ares (RHSA-2023:3662)

[241731](#) Red Hat Update for c-ares (RHSA-2023:3677)

[241735](#) Red Hat Update for c-ares (RHSA-2023:3741)

[241786](#) Red Hat Update for rh-nodejs14-nodejs (RHSA-2023:4039)

[241787](#) Red Hat Update for nodejs (RHSA-2023:4036)

[241788](#) Red Hat Update for nodejs:18 (RHSA-2023:4035)

[241790](#) Red Hat Update for nodejs:16 (RHSA-2023:4033)

[241792](#) Red Hat Update for nodejs:16 (RHSA-2023:4034)

257242 CentOS Security Update for c-ares (CESA-2023:3741)
284001 Fedora Security Update for c (FEDORA-2023-ae97529c00)
284101 Fedora Security Update for c (FEDORA-2023-520848815b)
355414 Amazon Linux Security Advisory for c-ares : ALAS2023-2023-198
355556 Amazon Linux Security Advisory for c-ares : ALAS-2023-1770
355588 Amazon Linux Security Advisory for c-ares : ALAS2-2023-2127
356117 Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2023-2023-344
356246 Amazon Linux Security Advisory for ecs-service-connect-agent : ALASECS-2023-007
356347 Amazon Linux Security Advisory for c-ares : AL2012-2023-450
356504 Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2ECS-2023-007
378619 Alibaba Cloud Linux Security Update for c-ares (ALINUX2-SA-2023:0028)
378623 Alibaba Cloud Linux Security Update for c-ares (ALINUX3-SA-2023:0052)
378787 F5 BIG-IP Denial of Service (DoS) Vulnerability (K000135831)
6000134 Debian Security Update for c-ares (DLA 3471-1)
673217 EulerOS Security Update for c-ares (EulerOS-SA-2023-2348)
673242 EulerOS Security Update for c-ares (EulerOS-SA-2023-2374)
673270 EulerOS Security Update for c-ares (EulerOS-SA-2023-2575)
673319 EulerOS Security Update for c-ares (EulerOS-SA-2023-2605)
673368 EulerOS Security Update for c-ares (EulerOS-SA-2023-2634)
673401 EulerOS Security Update for c-ares (EulerOS-SA-2023-2676)
673706 EulerOS Security Update for c-ares (EulerOS-SA-2023-3115)
710769 Gentoo Linux c-ares Multiple Vulnerabilities (GLSA 202310-09)
754046 SUSE Enterprise Linux Security Update for c-ares (SUSE-SU-2023:2313-1)
754083 SUSE Enterprise Linux Security Update for libcares2 (SUSE-SU-2023:2477-1)
754181 SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2023:2861-1)
906996 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (26913-1)
907015 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (26891-1)
907109 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (26937-1)
907282 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs18 (26939-1)

907567 Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (26918-1)
907724 Common Base Linux Mariner (CBL-Mariner) Security Update for python-gevent (26942-1)
941134 AlmaLinux Security Update for c-ares (ALSA-2023:3559)
941140 AlmaLinux Security Update for c-ares (ALSA-2023:3584)
941145 AlmaLinux Security Update for nodejs (ALSA-2023:3586)
941153 AlmaLinux Security Update for nodejs:18 (ALSA-2023:3577)
941168 AlmaLinux Security Update for nodejs:16 (ALSA-2023:4034)
941169 AlmaLinux Security Update for nodejs:18 (ALSA-2023:4035)
960941 Rocky Linux Security Update for c-ares (RLSA-2023:3559)
960945 Rocky Linux Security Update for nodejs:18 (RLSA-2023:3577)
960949 Rocky Linux Security Update for c-ares (RLSA-2023:3584)

© [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](#)