



# CVE-2023-31147

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

## Summary

<b>CVE</b>	CVE-2023-31147
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-05-25 22:15:00 UTC
<b>Updated</b>	2023-10-31 16:06:00 UTC
<b>Description</b>	c-ares is an asynchronous resolver library. When /dev/urandom or RtlGenRandom() are unavailable, c-ares uses rand() to

## Risk And Classification

**Problem Types:** CWE-330

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">C-ares Project</a>	<a href="#">C-ares</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All

## References

Reference	Source	Link	Tags
Insufficient randomness in generation of DNS query IDs · Advisory · c-ares/c-ares · GitHub	MISC	<a href="#">github.com</a>	
[SECURITY] Fedora 38 Update: c-ares-1.19.1-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproject.org</a>	
Release 1.19.1 · c-ares/c-ares · GitHub	MISC	<a href="#">github.com</a>	
c-ares: Multiple Vulnerabilities (GLSA 202310-09) — Gentoo security	MISC	<a href="#">security.gentoo.org</a>	
[SECURITY] Fedora 37 Update: c-ares-1.19.1-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">160732</a> Oracle Enterprise Linux Security Update for nodejs (ELSA-2023-3586)
<a href="#">160740</a> Oracle Enterprise Linux Security Update for 18 (ELSA-2023-3577)
<a href="#">160788</a> Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2023-4034)
<a href="#">160794</a> Oracle Enterprise Linux Security Update for nodejs:18 (ELSA-2023-4035)
<a href="#">161099</a> Oracle Enterprise Linux Security Update for c-ares (ELSA-2023-6635)
<a href="#">241702</a> Red Hat Update for nodejs:18 (RHSA-2023:3577)
<a href="#">241724</a> Red Hat Update for nodejs (RHSA-2023:3586)
<a href="#">241786</a> Red Hat Update for rh-nodejs14-nodejs (RHSA-2023:4039)
<a href="#">241787</a> Red Hat Update for nodejs (RHSA-2023:4036)
<a href="#">241788</a> Red Hat Update for nodejs:18 (RHSA-2023:4035)
<a href="#">241790</a> Red Hat Update for nodejs:16 (RHSA-2023:4033)
<a href="#">241792</a> Red Hat Update for nodejs:16 (RHSA-2023:4034)
<a href="#">242322</a> Red Hat Update for c-ares security (RHSA-2023:6635)
<a href="#">284001</a> Fedora Security Update for c (FEDORA-2023-ae97529c00)
<a href="#">284101</a> Fedora Security Update for c (FEDORA-2023-520848815b)
<a href="#">355414</a> Amazon Linux Security Advisory for c-ares : ALAS2023-2023-198
<a href="#">356117</a> Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2023-2023-344
<a href="#">356246</a> Amazon Linux Security Advisory for ecs-service-connect-agent : ALASECS-2023-007
<a href="#">356504</a> Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2ECS-2023-007
<a href="#">673270</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-2575)
<a href="#">673319</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-2605)
<a href="#">673489</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-2828)
<a href="#">673513</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-2833)
<a href="#">673706</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-3115)
<a href="#">673890</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-2780)
<a href="#">674117</a> EulerOS Security Update for c-ares (EulerOS-SA-2023-2804)
<a href="#">710769</a> Gentoo Linux c-ares Multiple Vulnerabilities (GLSA 202310-09)
<a href="#">754046</a> SUSE Enterprise Linux Security Update for c-ares (SUSE-SU-2023:2313-1)
<a href="#">754092</a> SUSE Enterprise Linux Security Update for libares (SUSE-SU-2023:2477-1)

<a href="#">754083</a> SUSE Enterprise Linux Security Update for libcares2 (SUSE-SU-2023:2477-1)
<a href="#">754181</a> SUSE Enterprise Linux Security Update for nodejs16 (SUSE-SU-2023:2861-1)
<a href="#">906992</a> Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (26869-1)
<a href="#">907007</a> Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (26847-1)
<a href="#">907092</a> Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (26874-1)
<a href="#">907312</a> Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs18 (26875-1)
<a href="#">907544</a> Common Base Linux Mariner (CBL-Mariner) Security Update for fluent-bit (26870-1)
<a href="#">941145</a> AlmaLinux Security Update for nodejs (ALSA-2023:3586)
<a href="#">941153</a> AlmaLinux Security Update for nodejs:18 (ALSA-2023:3577)
<a href="#">941168</a> AlmaLinux Security Update for nodejs:16 (ALSA-2023:4034)
<a href="#">941169</a> AlmaLinux Security Update for nodejs:18 (ALSA-2023:4035)
<a href="#">941381</a> AlmaLinux Security Update for c-ares (ALSA-2023:6635)
<a href="#">960945</a> Rocky Linux Security Update for nodejs:18 (RLSA-2023:3577)

© [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](#)