CVE-2022-4904

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-4904
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-06 23:15:00 UTC
Updated	2024-01-05 10:15:00 UTC
Description	A flaw was found in the c-ares package. The ares_set_sortlist is missing checks about the validity of the input string, which

Risk And Classification

Problem Types: CWE-1284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C-ares Project	C-ares	All	All	All	All
Application	C-ares Project	C-ares	-	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Software Collections	-	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 36 Update: c-ares-1.19.0-1.fc36 - package-announce - Fedora Mailing-Lists		lists
GLSA-202401-02		sec
[SECURITY] Fedora 36 Update: c-ares-1.19.0-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists
Potential stack overflow in ares_set_sortlist · Issue #496 · c-ares/c-ares · GitHub	MISC	gith
2168631 – (CVE-2022-4904) CVE-2022-4904 c-ares: buffer overflow in config_sortlist() due to missing string length check	MISC	bug
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160535 Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2023-1582)

160547 Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2023-1743)

160639 Oracle Enterprise Linux Security Update for nodejs:18 (ELSA-2023-2654)

160640 Oracle Enterprise Linux Security Update for nodejs and nodejs-nodemon (ELSA-2023-2655)

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

161099 Oracle Enterprise Linux Security Update for c-ares (ELSA-2023-6635)

161177 Oracle Enterprise Linux Security Update for c-ares (ELSA-2023-7116)

181580 Debian Security Update for c-ares (DLA 3323-1)

182005 Debian Security Update for c-ares (CVE-2022-4904)

199202 Ubuntu Security Notification for c-ares Vulnerability (USN-5907-1)

241304 Red Hat Update for nodejs:14 security (RHSA-2023:1533)

241332 Red Hat Update for nodejs:16 security (RHSA-2023:1582)

241341 Red Hat Update for nodejs:14 security (RHSA-2023:1742)

241342 Red Hat Update for nodejs:14 security (RHSA-2023:1743)

241343 Red Hat Update for rh-nodejs14-nodejs security (RHSA-2023:1744)

241429 Red Hat Update for nodejs and nodejs-nodemon security (RHSA-2023:2655)

241457 Red Hat Update for nodejs:18 security (RHSA-2023:2654)

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

242132 Red Hat Update for nodejs security (RHSA-2023:5533)

242277 Red Hat Update for c-ares (RHSA-2023:6291)

242322 Red Hat Update for c-ares security (RHSA-2023:6635)

242452 Red Hat Update for c-ares (RHSA-2023:7116)

242485 Red Hat Update for c-ares (RHSA-2023:7368)

242524 Red Hat Update for c-ares (RHSA-2023:7543)

283741 Fedora Security Update for c (FEDORA-2023-b121bd62a9)

283771 Fedora Security Update for c (FEDORA-2023-30e81e5293)

296100 Oracle Solaris 11.4 Support Repository Update (SRU) 58.144.3 Missing (CPUAPR2023)

355414 Amazon Linux Security Advisory for c-ares : ALAS2023-2023-198

355567 Amazon Linux Security Advisory for c-ares : ALAS-2023-1780

355622 Amazon Linux Security Advisory for nodejs : ALAS2023-2023-243

378467 Alibaba Cloud Linux Security Update for nodejs:14 (ALINUX3-SA-2023:0037)

672966 EulerOS Security Update for c-ares (EulerOS-SA-2023-1861)

672972 EulerOS Security Update for c-ares (EulerOS-SA-2023-1836)

673021 EulerOS Security Update for c-ares (EulerOS-SA-2023-1948)

673037 EulerOS Security Update for c-ares (EulerOS-SA-2023-1970)

673141 EulerOS Security Update for c-ares (EulerOS-SA-2023-2260)

673149 EulerOS Security Update for c-ares (EulerOS-SA-2023-2284)

710820 Gentoo Linux c-ares Multiple Vulnerabilities (GLSA 202401-02)

753783 SUSE Enterprise Linux Security Update for c-ares (SUSE-SU-2023:0486-1)

905703 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (13827)

905704 Common Base Linux Mariner (CBL-Mariner) Security Update for grpc (13818)

905706 Common Base Linux Mariner (CBL-Mariner) Security Update for python-gevent (13828)

905713 Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-mini_portile2 (13831)

905715 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (13817)

905723 Common Base Linux Mariner (CBL-Mariner) Security Update for grpc (13804)

905724 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (13803)

905726 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (13812)

905732 Common Base Linux Mariner (CBL-Mariner) Security Update for python-gevent (13813)

906758 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (13817-1)

906789 Common Base Linux Mariner (CBL-Mariner) Security Update for c-ares (13803-1)

907089 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs (13827-1)

907732 Common Base Linux Mariner (CBL-Mariner) Security Update for python-gevent (13828-1)

940976 AlmaLinux Security Update for nodejs:16 (ALSA-2023:1582)

940979 AlmaLinux Security Update for nodejs:14 (ALSA-2023:1743)

941013 AlmaLinux Security Update for nodejs and nodejs-nodemon (ALSA-2023:2655)

941013 AlmaLinux Security Update for nodejs and nodejs-nodemon (ALSA-2023:2655)

941014 AlmaLinux Security Update for nodejs:18 (ALSA-2023:2654)

941169 AlmaLinux Security Update for nodejs:18 (ALSA-2023:4035)

941381 AlmaLinux Security Update for c-ares (ALSA-2023:6635)

941458 AlmaLinux Security Update for c-ares (ALSA-2023:7116)

960902 Rocky Linux Security Update for nodejs:16 (RLSA-2023:1582)

960917 Rocky Linux Security Update for nodejs:14 (RLSA-2023:1743)

960937 Rocky Linux Security Update for nodejs and nodejs-nodemon (RLSA-2023:2655)