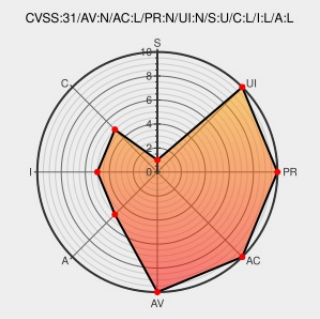
CVE-2021-3672

Published on: 11/23/2021 12:00:00 AM UTC

Last Modified on: 11/26/2021 07:06:00 PM UTC

CVE-2021-3672

Source: Mitre | Source: Nist | Print: PDF



Certain versions of C-ares from C-ares Project contain the following vulnerability:

A flaw was found in c-ares library, where a missing input validation check of host names returned by DNS (Domain Name Servers) can lead to output of wrong hostnames which might potentially lead to Domain Hijacking. The highest threat from this vulnerability is to confidentiality and integrity as well as system availability.

CVE-2021-3672 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.3 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	LOW

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Missing input validation on hostnames returned by DNS servers	c-ares.haxx.se text/html	MISC c-ares.haxx.se/adv_20210810.html
1988342 – (CVE-2021-3672) CVE-2021-3672 c-ares: Missing input validation of	bugzilla.redhat.com	MISC

host names may lead to domain hijacking

text/html

bugzilla.redhat.com/show_bug.cgi?id=1988342

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

159398 Oracle Enterprise Linux Security Update for nodejs:12 (ELSA-2021-3623)

159408 Oracle Enterprise Linux Security Update for nodejs:14 (ELSA-2021-3666)

178750 Debian Security Update for c-ares (DSA 4954-1)

178751 Debian Security Update for c-ares (DLA 2738-1)

198455 Ubuntu Security Notification for c-ares vulnerability (USN-5034-1)

239590 Red Hat Update for rh-nodejs12-nodejs and rh-nodejs12-nodejs-nodemon (RHSA-2021:3281)

239591 Red Hat Update for rh-nodejs14-nodejs and rh-nodejs14-nodejs-nodemon (RHSA-2021:3280)

239645 Red Hat Update for nodejs:12 (RHSA-2021:3623)

239654 Red Hat Update for nodejs:12 (RHSA-2021:3639)

239655 Red Hat Update for nodejs:12 (RHSA-2021:3638)

239658 Red Hat Update for nodejs:14 (RHSA-2021:3666)

281816 Fedora Security Update for c (FEDORA-2021-0a60cbb948)

281821 Fedora Security Update for mingw (FEDORA-2021-001ec24fc5)

281822 Fedora Security Update for mingw (FEDORA-2021-c83b66abdb)

281869 Fedora Security Update for c (FEDORA-2021-52c89b44a9)

352861 Amazon Linux Security Advisory for c-ares: ALAS-2021-1545

375877 Kibana Multiple Security Vulnerabilities (ESA-2021-21, ESA-2021-22, ESA-2021-24)

376035 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Node.js Vulnerabilities (K53225395)

670816 EulerOS Security Update for c-ares (EulerOS-SA-2021-2704)

670983 EulerOS Security Update for c-ares (EulerOS-SA-2021-2679)

670989 EulerOS Security Update for c-ares (EulerOS-SA-2021-2652)

671016 EulerOS Security Update for c-ares (EulerOS-SA-2021-2623)

671035 EulerOS Security Update for c-ares (EulerOS-SA-2021-2574)

750967 SUSE Enterprise Linux Security Update for libcares2 (SUSE-SU-2021:2690-1)

750975 SUSE Enterprise Linux Security Update for c-ares (SUSE-SU-2021:2760-1)

750979 OpenSUSE Security Update for c-ares (openSUSE-SU-2021:2760-1)

751022 OpenSUSE Security Update for c-ares (openSUSE-SU-2021:1168-1)

751061 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:2875-1)

751071 OpenSUSE Security Update for nodejs12 (openSUSE-SU-2021:1214-1)

751093 OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:2953-1)

751112 OpenSUSE Security Update for nodejs10 (openSUSE-SU-2021:1239-1)

751171 OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:3211-1)

751178 OpenSUSE Security Update for nodejs14 (openSUSE-SU-2021:1313-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C-ares Project	C-ares	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.7	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Computer Node	1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.1	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.1	All	All	All

Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.1	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Tus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	1	All	All	All

cpe:2.3:a:c-ares_project:c-ares:*:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_computer_node:1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:7.7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_ibm_z_systems:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_ibm_z_systems_eus:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_ibm_z_systems_eus:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_ibm_z_systems_eus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_ibm_z_systems_eus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_power_little_endian:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_power_little_endian_eus:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_power_little_endian_eus:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_for_power_little_endian_eus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_tus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_update_services_for_sap_solutions:8.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_update_services_for_sap_solutions:8.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_update_services_for_sap_solutions:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_tus:8.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@matteocollina	More specifically, in nodejs.org/en/blog/releas… CVE-2021-3672 is all about DNS. twitter.com/matteocollina/…	2021-08-11 17:02:51
@attritionorg	@JesscaHaworth In bit.ly/37Mq6jg you say "The first vulnerability (CVE-2021-3672/CVE-2021-2293) is". 3672… twitter.com/i/web/status/1…	2021-08-15 15:23:33

← Previous ID

Next ID→