



CVE-2022-0324

Published on: Not Yet Published

Last Modified on: 11/17/2022 11:16:00 PM UTC

CVE-2022-0324

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Software For Open Networking In The Cloud](#) from [Linuxfoundation](#) contain the following vulnerability:

There is a vulnerability in DHCPv6 packet parsing code that could be explored by remote attacker to craft a packet that could cause buffer overflow in a memcpy call, leading to out-of-bounds memory write that would cause dhcp6relay to crash. Dhcp6relay is a critical process and could cause dhcp relay docker to shutdown. Discovered by Eugene

Lim of GovTech Singapore.

CVE-2022-0324 has been assigned by cve_disclosure@tech.gov.sg to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Linux Foundation - Software for Open Networking in the Cloud (SONiC)** version = 202111

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Dhcp6relay Buffer Overflow Vulnerability · Advisory · sonic-net/sonic-buildimage · GitHub	github.com text/html	MISC github.com/sonic-net/sonic-buildimage/security/advisories/GHSA-m4qf-8rrq-mph9
CVE-2022-0324 GovTech CSG Security Advisories	govtech-csg.github.io text/html	MISC govtech-csg.github.io/security-advisories/2022/11/14/CVE-2022-0324.html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Software For Open Networking In The Cloud	202111	All	All	All
cpe:2.3:a:linuxfoundation:software_for_open_networking_in_the_cloud:202111:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-0324 : There is a vulnerability in DHCPv6 packet parsing code that could be explored by remote attacker to... twitter.com/i/web/status/1...	2022-11-14 17:03:51
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-0324 There is a vulnerability in DHCPv6 packet parsing code that could... twitter.com/i/web/status/1...	2022-11-14 17:55:55

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)