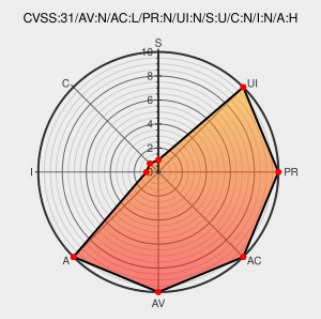
CVE-2022-0324

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

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→