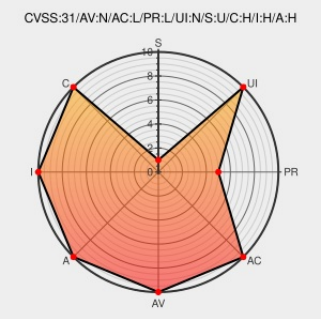
CVE-2020-11498

Published on: 04/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:24 PM UTC

CVE-2020-11498

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nebula from Slack contain the following vulnerability:

Slack Nebula through 1.1.0 contains a relative path vulnerability that allows a low-privileged attacker to execute code in the context of the root user via tun_darwin.go or tun_windows.go. A user can also use Nebula to execute arbitrary code in the user's own context, e.g., for user-level persistence or to bypass security controls. NOTE: the vendor states that this "requires a high degree of access and other preconditions that are tough to achieve."

CVE-2020-11498 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
use absolute paths on darwin and windows by wadey · Pull	Patch	MISC:github.com/slackhq/nebula/pull/191

use absolute paths on darwin and windows by wadey · Pull Request #191 · slackhq/nebula · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/slackhq/nebula/pull/191
Slack Nebula - Relative Path Bug Bounty Disclosure (Med: $750) « pwn3d.org	Exploit Third Party Advisory www.pwn3d.org text/html	MISC www.pwn3d.org/posts/7918501-slack-nebula-relative-path-bug-bounty-disclosure

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	Slack	Nebula	All	All	All	All

cpe:2.3:a:slack:nebula:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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 registred 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