



CVE-2021-21382

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-21382
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-11 21:15:00 UTC
Updated	2022-10-21 22:44:00 UTC
Description	Restund is an open source NAT traversal server. The restund TURN server can be instructed to open a relay to the loopback

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wire	Restund	All	All	All	All

References

Reference
ansible-restund/restund.conf.j2 at master · wireapp/ansible-restund · GitHub
turn: block forwarding to loopback/any by z-dule · Pull Request #7 · wireapp/restund · GitHub
TALOS-2018-0732 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
Unsafe loopback forwarding interface · Advisory · wireapp/restund · GitHub
Details about CVE-2020-26262, bypass of Coturn's default access control protection Communication Breakdown - real-time communications
Loopback bypass by using 0.0.0.0, [::1] or [::] as the peer address · Advisory · coturn/coturn · GitHub
Restund (TURN) servers — Wire documentation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)