



CVE-2021-32593

Published on: Not Yet Published

Last Modified on: 04/13/2022 06:59:00 PM UTC

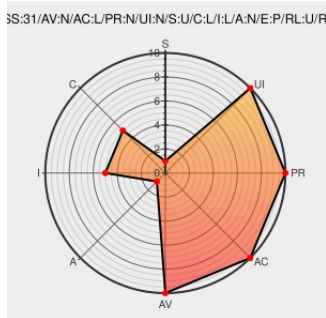
CVE-2021-32593

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Fortiwan** from **Fortinet** contain the following vulnerability:

A use of a broken or risky cryptographic algorithm vulnerability [CWE-327] in the Dynamic Tunnel Protocol of FortiWAN before 4.5.9 may allow an unauthenticated remote attacker to decrypt and forge protocol communication messages.

CVE-2021-32593 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Fortinet FortiWAN** version **FortiWAN before 4.5.9**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
PSIRT Advisories FortiGuard	fortiguard.com text/html	CONFIRM fortiguard.com/psirt/FG-IR-21-070

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	Fortinet	Fortiwan	All	All	All	All
cpe:2.3:a:fortinet:fortiwan:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-32593 : A use of a broken or risky cryptographic algorithm vulnerability [CWE-327] in the Dynamic Tunnel P... twitter.com/i/web/status/1...	2022-04-06 09:25:37
 /r/netcve	CVE-2021-32593	2022-04-06 10:38:09

[← 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](#)