



CVE-2021-44171

Published on: Not Yet Published

Last Modified on: 10/12/2022 06:45:00 PM UTC

CVE-2021-44171

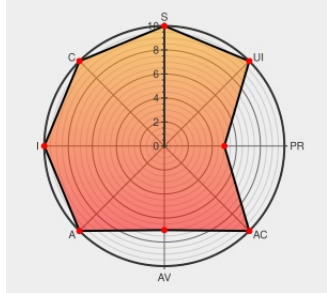
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

SS:31/AV:A/C:L/PR:L/UI:N/S:C/C:H/I/H/A/H/E:F/RL:X/R



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

A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiOS version 6.0.0 through 6.0.14, FortiOS version 6.2.0 through 6.2.10, FortiOS version 6.4.0 through 6.4.8, FortiOS version 7.0.0 through 7.0.3 allows attacker to execute privileged commands on a linked FortiSwitch via diagnostic CLI commands.

CVE-2021-44171 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **FortiOS 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.10, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.14, 6.0.13, 6.0.12, 6.0.11, 6.0.10, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0**

CVSS3 Score: **8 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

ADJACENT_NETWORK

LOW

LOW

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

HIGH

HIGH

CVE References

Description

Tags

Link

PSIRT Advisories | FortiGuard

[fortiguard.com](https://fortiguard.com/text/html)
[text/html](https://fortiguard.com/text/html)

CONFIRM fortiguard.com/psirt/FG-IR-21-242

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.

Related QID Numbers

[43933](#) FortiOS - Privilege Escalation Vulnerability via switch-control CLI command (FG-IR-21-242)

[44046](#) FortiOS - Privilege Escalation Vulnerability via switch-control CLI command (FG-IR-21-242) (Unauthenticated Check)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
cpe:2.3:o:fortinet:fortios:*****:						
cpe:2.3:o:fortinet:fortios:*****:						
cpe:2.3:o:fortinet:fortios:*****:						
cpe:2.3:o:fortinet:fortios:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-44171 A improper neutralization of special elements used in an os comma... twitter.com/i/web/status/1...	2022-10-10 12:56:02
 @CVEreport	CVE-2021-44171 : A improper neutralization of special elements used in an os command 'os command injection' in Fo... twitter.com/i/web/status/1...	2022-10-10 14:03:09
 /r/netcve	CVE-2021-44171	2022-10-10 14:38:40

[← Previous ID](#)

[Next ID →](#)

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](#)