



CVE-2021-44170

Published on: Not Yet Published

Last Modified on: 07/25/2022 05:05:00 PM UTC

CVE-2021-44170

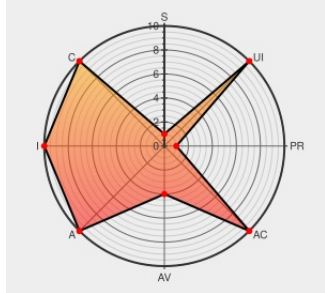
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

IS:31/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/R



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

A stack-based buffer overflow vulnerability [CWE-121] in the command line interpreter of FortiOS before 7.0.4 and FortiProxy before 2.0.8 may allow an authenticated attacker to execute unauthorized code or commands via specially crafted command line arguments.

CVE-2021-44170 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiProxy**, **FortiOS** version **FortiOS before 7.0.4**; **FortiProxy** before 2.0.8

CVSS3 Score: **6.7 - MEDIUM**

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

CVE References

Description	Tags	Link
PSIRT Advisories FortiGuard	fortiguard.com text/html	CONFIRM fortiguard.com/psirt/FG-IR-21-179

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

43910 FortiOS Stack-Based Buffer Overflow Vulnerability (FG-IR-21-179)

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
Application	Fortinet	Fortiproxy	All	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All
Application	Fortinet	Fortiproxy	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:a:fortinet:fortiproxy:*:*:*:*:*.*						
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*.*						
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*.*						
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @sidfm_jp	Fortinet FortiOS の診断 CLI コマンドの処理に任意のコードを実行される問題 (CVE-2021-44170) [42687] sid.softek.jp/content/show/4... #SIDfm #脆弱性情報	2022-07-06 08:00:09
 @CVEreport	CVE-2021-44170 : A stack-based buffer overflow vulnerability [CWE-121] in the command line interpreter of FortiOS b... twitter.com/i/web/status/1...	2022-07-18 16:42:48
 /r/netcve	CVE-2021-44170	2022-07-18 17:38:35

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](#)