

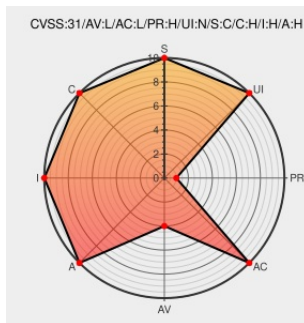


CVE-2022-42476

Published on: Not Yet Published

Last Modified on: 03/14/2023 07:31:00 PM UTC

CVE-2022-42476

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Fortios](#) from [Fortinet](#) contain the following vulnerability:

A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2, 7.0.0 through 7.0.8 and before 6.4.11, FortiProxy version 7.2.0 through 7.2.2 and 7.0.0 through 7.0.8 allows privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests.

CVE-2022-42476 has been assigned by [psirt@fortinet.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.2 - HIGH**

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

CVE References

Description	Tags	Link
PSIRT Advisories FortiGuard	fortiguard.com text/html	MISC fortiguard.com/psirt/FG-IR-22-401

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

[43994](#) FortiOS Path Traversal Vulnerability (FG-IR-22-401)

[44058](#) FortiOS Path Traversal Vulnerability (FG-IR-22-401) (Unauthenticated Check)

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
Application	Fortinet	Fortiproxy	7.2.0	All	All	All
Application	Fortinet	Fortiproxy	7.2.1	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:o:fortinet:fortios:*:*:*:*:*:
```

```
cpe:2.3:a:fortinet:fortiproxy:7.2.0:*:*:*:*:*:
```

```
cpe:2.3:a:fortinet:fortiproxy:7.2.1:*:*:*:*:*:
```

```
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)
 @CVEreport	CVE-2022-42476 : A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.2,... twitter.com/i/web/status/1...	2023-03-07 17:08:12
 /r/netcve	CVE-2022-42476	2023-03-07 17:38:57

 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Fortinet Products Could Allow for Arbitrary Code Execution - PATCH NOW	2023-03-09 13:44:23
 /r/k12cybersecurity	UPDATED - MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Fortinet Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2023-03-14 16:50:34

[← 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](#)