



CVE-2022-26121

Published on: Not Yet Published

Last Modified on: 10/12/2022 06:44:00 PM UTC

CVE-2022-26121

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

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



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

An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager GUI 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11 may allow an unauthenticated and remote attacker to access report template images via referencing the name in the URL path.

CVE-2022-26121 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Fortinet - Fortinet FortiManager, FortiAnalyzer** version **FortiManager 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11; FortiAnalyzer 7.0.0 through 7.0.3, 6.4.0 through 6.4.8, 6.2.0 through 6.2.9, 6.0.0 through 6.0.11, 5.6.0 through 5.6.11**

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

NONE

NONE

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

LOW

NONE

NONE

CVE References

Description

Tags

Link

PSIRT Advisories | FortiGuard

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

CONFIRM fortiguard.com/psirt/FG-IR-22-026

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 CVE Numbers

Related QID Numbers

377696 FortiAnalyzer and FortiManager - Improper Authorization Vulnerability (FG-IR-22-026)

43934 FortiAnalyzer and FortiManager - improper authorization to template image (FG-IR-22-026)

Known Affected Configurations (CPE V2.3)

[illegible]

```
cpe:2.3:a:fortinet:fortianalyzer:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:fortinet:fortianalyzer:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:fortinet:fortianalyzer:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:fortinet:fortianalyzer:*****:*.*.:
```

```
cpe:2.3:a:fortinet:fortianalyzer:*****:
```

```
cpe:2.3:a:fortinet:fortimanager:*.*.*.*.*.*.:
```

```
cpe:2.3:a:fortinet:fortimanager:*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:fortinet:fortimanager:*.*.*.*.*.*.:
```

```
cpe:2.3:a:fortinet:fortimanager:*.*.*.*.*.*.:
```

```
cpe:2.3:a:fortinet:fortimanager:*.*.*.*.*.*.:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-26121 : An exposure of resource to wrong sphere vulnerability [CWE-668] in FortiAnalyzer and FortiManager... twitter.com/i/web/status/1...	2022-10-10 14:07:08
 /r/netcve	CVE-2022-26121	2022-10-10 15:38:46

© [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](#)