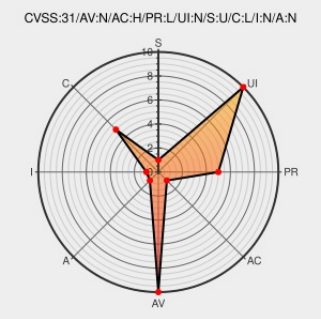
CVE-2023-23776

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:07:00 AM UTC

CVE-2023-23776

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fortianalyzer from Fortinet contain the following vulnerability:

An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiAnalyzer versions 7.2.0 through 7.2.1, 7.0.0 through 7.0.4 and 6.4.0 through 6.4.10 may allow a remote authenticated attacker to read the client machine password in plain text in a heartbeat response when a log-fetch request is made from the FortiAnalyzer

CVE-2023-23776 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **Fortinet** - **FortiAnalyzer** version **<= 7.2.1**

Affected Vendor/Software: **Fortinet** - **FortiAnalyzer** version **<= 7.0.4**

Affected Vendor/Software: **Fortinet** - **FortiAnalyzer** version **<= 6.4.10**

CVSS3 Score: 3.1 - LOW

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

CVE References

Description	Tags	Link
PSIRT Advisories | FortiGuard	fortiguard.com text/html	MISC fortiguard.com/psirt/FG-IR-22-447

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

378068 Fortinet FortiAnalyzer Information Disclosure Vulnerability (FG-IR-22-447)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortianalyzer	All	All	All	All

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-23776 : An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiAnal… twitter.com/i/web/status/1…	2023-03-07 17:09:08
/r/netcve	CVE-2023-23776	2023-03-07 17:38:58
/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 2024 | |
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 registred 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