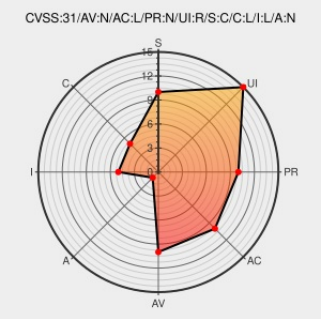
CVE-2020-12811

Published on: 09/24/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:36 PM UTC

CVE-2020-12811

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



Certain versions of Fortianalyzer from Fortinet contain the following vulnerability:

An improper neutralization of script-related HTML tags in a web page in FortiManager 6.2.0, 6.2.1, 6.2.2, and 6.2.3and FortiAnalyzer 6.2.0, 6.2.1, 6.2.2, and 6.2.3 may allow an attacker to execute a cross site scripting (XSS) via the Identify Provider name field.

CVE-2020-12811 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 6.2.0, 6.2.1, 6.2.2, and 6.2.3 ; FortiAnalyzer 6.2.0, 6.2.1, 6.2.2, and 6.2.3**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
XSS vulnerability in FortiManager and FortiAnalyzer | FortiGuard	Vendor Advisory fortiguard.com	CONFIRM fortiguard.com/advisory/FG-IR-20-005

text/html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

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

cpe:2.3:a:fortinet:fortimanager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report