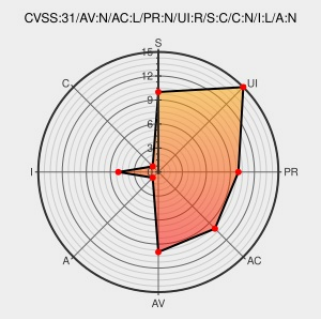
CVE-2020-15937

Published on: 03/03/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-15937

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



Certain versions of Fortios from Fortinet contain the following vulnerability:

An improper neutralization of input vulnerability in FortiGate version 6.2.x below 6.2.5 and 6.4.x below 6.4.1 may allow a remote attacker to perform a stored cross site scripting attack (XSS) via the IPS and WAF logs dashboard.

CVE-2020-15937 has been assigned by psirt@fortinet.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Fortinet** - **Fortinet FortiOS** version **FortiOS 6.4.1, 6.2.5**

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 observed in Log and Report section of FortiGate | FortiGuard	Not Applicable Vendor Advisory fortiguard.com	CONFIRM fortiguard.com/advisory/FG-IR-20-068

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.

Related QID Numbers

44094 FortiOS - Cross Site Scripting (XSS) Vulnerability (FG-IR-20-068)

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

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→