



CVE-2019-5590

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-5590
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-28 17:15:00 UTC
Updated	2019-09-03 17:36:00 UTC
Description	The URL part of the report message is not encoded in Fortinet FortiWeb 6.0.2 and below which may allow an attacker to ex

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Fortinet Fortiweb CVE-2019-5590 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
Cross-Site-Scripting (XSS) vulnerability in Fortiweb reports FortiGuard	CONFIRM	fortiguard.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

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