CVE-2015-1459

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-1459
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-03 16:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Fortinet FortiAuthenticator 3.0.0 allows remote attackers to inject arbitrary web sc

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fortinet	Fortiauthenticator	3.0.0	All	All	All
Application	Fortinet	Fortiauthenticator	3.0.0	All	All	All

References

Reference	Source	Lin
IBM X-Force Exchange	XF	exc
FortiGuard.com | FortiAuthenticator multiple vulnerabilities	CONFIRM	ww
Fortinet FortiAuthenticator Appliance Multiple Security Vulnerabilities	BID	ww
Security Advisory SA62836 - Fortinet FortiAuthenticator "operation" Cross-Site Scripting Vulnerability - Secunia	SECUNIA	sec
Fortinet FortiAuthenticator XSS / Disclosure / Bypass ≈ Packet Storm	MISC	pac
Risks in POS Systems: The Importance of a Security Assessment	MISC	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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