CVE-2019-10261

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

Summary

CVE	CVE-2019-10261
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-03 15:29:00 UTC
Updated	2019-05-06 17:03:00 UTC
Description	CentOS Web Panel (CWP) 0.9.8.789 is vulnerable to Stored/Persistent XSS for the "Name Server 1" and "Name Server 2"

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Centos-webpanel	Centos Web Panel	0.9.8.789	All	All	All
Operating System	Centos-webpanel	Centos Web Panel	0.9.8.789	All	All	All

References

Reference	Source	Link
CentOS Web Panel CVE-2019-10261 Multiple HTML Injection Vulnerabilities	BID	www.securityfocu
CentOS Web Panel 0.9.8.789 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecu
CentOS Web Panel 0.9.8.789 - NameServer Field Persistent Cross-Site Scripting - Linux webapps Exploit	EXPLOIT-DB	www.exploit-db.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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