CVE-2006-0800

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

Summary

CVE	CVE-2006-0800
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-20 22:02:00 UTC
Updated	2017-07-20 01:30:00 UTC
Description	Interpretation conflict in PostNuke 0.761 and earlier allows remote attackers to conduct cross-site scripting (XSS) attacks vi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postnuke Software Foundation	Postnuke	0.62	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.63	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.64	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.7	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.70	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.703	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.71	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.72	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.721	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.726.3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.73	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.74	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.75	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.75_rc3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.761	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.761a	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.76_rc4	All	All	All

Application	Postnuke Software Foundation	Postnuke	0.76_rc4a	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.76_rc4b	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.62	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.63	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.64	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.7	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.70	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.703	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.71	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.72	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.721	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.726.3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.73	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.74	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.75	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.75_rc3	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.761	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.761a	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.76_rc4	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.76_rc4a	All	All	All
Application	Postnuke Software Foundation	Postnuke	0.76_rc4b	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Vendor Advisory
News index page :: PostNuke :: Flexible Content Management System	CONFIRM	news.postnuke.com	Patch
PostNuke Multiple Input Validation Vulnerabilities	BID	www.securityfocus.com	Exploit, Patch
PostNuke Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com	Patch, Vendor Advis
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FULLDISC	archives.neohapsis.com	
SecurityReason - Multiple vulnerabilities in PostNuke <= 0.761	SREASON	securityreason.com	
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.

Free CVE JSON API cve.report/api

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