



CVE-2002-1996

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

Summary

CVE	CVE-2002-1996
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Cross-site scripting (XSS) vulnerability in PostNuke 0.71 and earlier allows remote attackers to inject arbitrary web script or

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

AV:N/AC:H/Au:N/C:N/I:P/A:N

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:H/Au:N/C:N/I:P/A:N

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

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References	
Reference	Source
Neohapsis Archives - Bugtraq - Re: PostNuke Bugged - From rootkiddemail.com	af854a3a-2127-4221
ISS X-Force Database: postnuke-modules-index-css (8605): PostNuke modules.php and index.php cross-site scripting	af854a3a-2127-4221
PostNuke Cross Site Scripting Vulnerability	af854a3a-2127-4221
Neohapsis Archives - Bugtraq - PostNuke Bugged - From rootkidd@email.com	af854a3a-2127-4221
SourceForge.net: Log In to SourceForge.net	af854a3a-2127-4221
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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