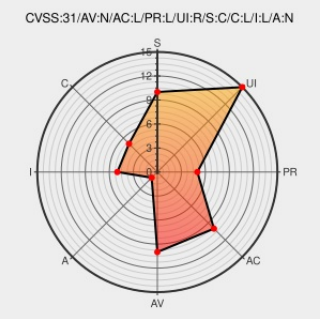
CVE-2022-46889

Published on: Not Yet Published

Last Modified on: 01/25/2023 07:42:00 PM UTC

CVE-2022-46889

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nexusphp from Nexusphp contain the following vulnerability:

A persistent cross-site scripting (XSS) vulnerability in NexusPHP before 1.7.33 allows remote authenticated attackers to permanently inject arbitrary web script or HTML via the title parameter used in /subtitles.php.

CVE-2022-46889 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
NexusPHP - SureCloud Security Review Identifies Authenticated and Unauthenticated Vulnerabilities	www.surecloud.com text/html	MISC www.surecloud.com/resources/blog/nexusphp-surecloud-security-review-identifies-authenticated-unauthenticated-vulnerabilities
Release v1.7.33 · xiaomlove/nexusphp · GitHub	github.com text/html	MISC github.com/xiaomlove/nexusphp/releases/tag/v1.7.33

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A persistent cross-site scripting (XSS) vulnerability in NexusPHP before 1.7.33 allows remote authenticated attackers…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nexusphp	Nexusphp	All	All	All	All

cpe:2.3:a:nexusphp:nexusphp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-46889 : A persistent cross-site scripting #XSS vulnerability in NexusPHP before 1.7.33 allows remote aut… twitter.com/i/web/status/1…	2023-01-19 19:05:10
/r/netcve	CVE-2022-46889	2023-01-19 19:39:46

← Previous ID

Next ID→