



# Nexus Repository 3 - Reflected Cross-Site Scripting (XSS) in ?describe Pages

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-3438
<b>State</b>	PUBLISHED
<b>Assigner</b>	Sonatype
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 23:16:59 UTC
<b>Updated</b>	2026-04-13 15:02:47 UTC
<b>Description</b>	A reflected cross-site scripting vulnerability exists in Sonatype Nexus Repository versions 3.0.0 through 3.90.2 that allows u

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from 103e4ec9-0a87-450b-af77-479448ddef11

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.002300000 probability, percentile 0.457940000 (date 2026-04-12)

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	103e4ec9-0a87-450b-af77-479448ddef11	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Active

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Sonatype</a>	<a href="#">Nexus Repository</a>	affected 3.0.0 3.91.0 semver	Not specified

### References

Reference	Source	Link
<a href="https://support.sonatype.com/hc/en-us/articles/50609137161363">support.sonatype.com/hc/en-us/articles/50609137161363</a>	103e4ec9-0a87-450b-af77-479448ddef11	<a href="https://support.sonatype.com/hc/en-us/articles/50609137161363">support.sonatype.c</a>
<a href="https://help.sonatype.com/en/sonatype-nexus-repository-3-91-0-release-notes.html">help.sonatype.com/en/sonatype-nexus-repository-3-91-0-release-notes.html</a>	103e4ec9-0a87-450b-af77-479448ddef11	<a href="https://help.sonatype.com/en/sonatype-nexus-repository-3-91-0-release-notes.html">help.sonatype.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)