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

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

Summary

CVE	CVE-2026-3438
State	PUBLISHED
Assigner	Sonatype
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 23:16:59 UTC
Updated	2026-04-13 15:02:47 UTC
Description	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/MSC:X/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/MSC:X/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	Sonatype	Nexus Repository	affected 3.0.0 3.91.0 semver	Not specified

References

Reference	Source	Link
support.sonatype.com/hc/en-us/articles/50609137161363	103e4ec9-0a87-450b-af77-479448ddef11	support.sonatype.c
help.sonatype.com/en/sonatype-nexus-repository-3-91-0-release-notes.html	103e4ec9-0a87-450b-af77-479448ddef11	help.sonatype.com
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.