



# Stored cross-site scripting in Pending Changes sidebar

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

## Summary

<b>CVE</b>	CVE-2026-20915
<b>State</b>	PUBLISHED
<b>Assigner</b>	Checkmk
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 15:16:11 UTC
<b>Updated</b>	2026-04-02 12:06:00 UTC
<b>Description</b>	Stored cross-site scripting (XSS) in Checkmk version 2.5.0 (beta) before 2.5.0b2 allows authenticated users with permission

## Risk And Classification

**Primary CVSS:** v4.0 8.5 HIGH from security@checkmk.com

**CVSS:**4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:H/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:** 0.000430000 probability, percentile 0.132140000 (date 2026-04-01)

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

Version	Source	Type	Score	Severity	Vector
4.0	security@checkmk.com	Secondary	8.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:L/SA:N
4.0	CNA	DECLARED	8.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:H/SC:N/SI:L/SA:N
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Passive

CVSS

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:H/VA:H/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkmk	Checkmk	2.5.0	b1	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Checkmk GmbH	Checkmk	affected 2.5.0b1 2.5.0b2 semver	Not specified

## References

Reference	Source	Link	Tags
<a href="https://checkmk.com/werk/19526">checkmk.com/werk/19526</a>	<a href="mailto:security@checkmk.com">security@checkmk.com</a>	<a href="https://checkmk.com">checkmk.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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