Stored cross-site scripting in Pending Changes sidebar

MITRE | NVD | CVE.ORG | Print: PDF

Summary

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

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/MSC:X/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

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/MSC:X/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
checkmk.com/werk/19526	security@checkmk.com	checkmk.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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