Insufficient permission validation on multiple REST API Quick Setup endpoints

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-24096
State	PUBLISHED
Assigner	Checkmk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 11:15:58 UTC
Updated	2026-04-01 14:23:37 UTC
Description	Insufficient permission validation on multiple REST API Quick Setup endpoints in Checkmk 2.5.0 (beta) before version 2.5.(

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from security@checkmk.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/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: 0.000380000 probability, percentile 0.115300000 (date 2026-04-01)

Problem Types: CWE-280 | CWE-280 CWE-280: Improper Handling of Insufficient Permissions or Privileges

Version	Source	Type	Score	Severity	Vector
4.0	security@checkmk.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/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	Checkmk GmbH	Checkmk	affected 2.5.0b1 2.5.0b2 semver	Not specified
CNA	Checkmk GmbH	Checkmk	affected 2.4.0 2.4.0p25 semver	Not specified

References

Reference	Source	Link	Tags
checkmk.com/werk/18989	security@checkmk.com	checkmk.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: PS Positive Security GmbH (en)

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

CVE.report and Source URL Uptime Status status.cve.report