Potential livestatus injection in notification test

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

Summary

CVE	CVE-2026-33456
State	PUBLISHED
Assigner	Checkmk
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 09:16:24 UTC
Updated	2026-04-20 17:10:06 UTC
Description	Livestatus injection in the notification test mode in Checkmk <2.5.0b4 and <2.4.0p26 allows an authenticated user with acce

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from security@checkmk.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/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: 0.000410000 probability, percentile 0.124100000 (date 2026-04-21)

Problem Types: CWE-140 | CWE-140 CWE-140: Improper Neutralization of Delimiters

Version	Source	Type	Score	Severity	Vector
4.0	security@checkmk.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

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:H/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Checkmk	Checkmk	2.4.0	-	All	All
Application	Checkmk	Checkmk	2.4.0	b1	All	All
Application	Checkmk	Checkmk	2.4.0	b2	All	All
Application	Checkmk	Checkmk	2.4.0	b3	All	All
Application	Checkmk	Checkmk	2.4.0	b4	All	All

Application	Checkmk	Checkmk	2.4.0	b5	All	All
Application	Checkmk	Checkmk	2.4.0	b6	All	All
Application	Checkmk	Checkmk	2.4.0	p1	All	All
Application	Checkmk	Checkmk	2.4.0	p10	All	All
Application	Checkmk	Checkmk	2.4.0	p11	All	All
Application	Checkmk	Checkmk	2.4.0	p12	All	All
Application	Checkmk	Checkmk	2.4.0	p13	All	All
Application	Checkmk	Checkmk	2.4.0	p14	All	All
Application	Checkmk	Checkmk	2.4.0	p15	All	All
Application	Checkmk	Checkmk	2.4.0	p16	All	All
Application	Checkmk	Checkmk	2.4.0	p17	All	All
Application	Checkmk	Checkmk	2.4.0	p18	All	All
Application	Checkmk	Checkmk	2.4.0	p19	All	All
Application	Checkmk	Checkmk	2.4.0	p2	All	All
Application	Checkmk	Checkmk	2.4.0	p20	All	All
Application	Checkmk	Checkmk	2.4.0	p21	All	All
Application	Checkmk	Checkmk	2.4.0	p22	All	All
Application	Checkmk	Checkmk	2.4.0	p23	All	All
Application	Checkmk	Checkmk	2.4.0	p24	All	All
Application	Checkmk	Checkmk	2.4.0	p25	All	All
Application	Checkmk	Checkmk	2.4.0	p3	All	All
Application	Checkmk	Checkmk	2.4.0	p4	All	All
Application	Checkmk	Checkmk	2.4.0	p5	All	All
Application	Checkmk	Checkmk	2.4.0	p6	All	All
Application	Checkmk	Checkmk	2.4.0	p7	All	All
Application	Checkmk	Checkmk	2.4.0	p8	All	All
Application	Checkmk	Checkmk	2.4.0	p9	All	All
Application	Checkmk	Checkmk	2.5.0	b1	All	All
Application	Checkmk	Checkmk	2.5.0	b2	All	All
Application	Checkmk	Checkmk	2.5.0	b3	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Checkmk GmbH	Checkmk	affected 2.5.0 2.5.0b4 semver	Not specified
CNA	Checkmk GmbH	Checkmk	affected 2.4.0 2.4.0p26 semver	Not specified

References

Reference	Source	Link	Tags
checkmk.com/werk/17989	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.

© 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 registred 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

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