Wazuh GitHub Actions Workflow Exposure of Sensitive Credentials

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-15617
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 18:16:03 UTC
Updated	2026-03-31 17:58:15 UTC
Description	Wazuh version 4.12.0 contains an exposure vulnerability in GitHub Actions workflow artifacts that allows attackers to extrac

Risk And Classification

Primary CVSS: v4.0 8.3 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:H/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 0.125570000 (date 2026-04-01)

Problem Types: CWE-522 | CWE-522 CWE-522 Insufficiently Protected Credentials

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.3	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/S/
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:N/S/
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	disclosure@vulncheck.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:L
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:L

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wazuh	Wazuh	4.12.0	All	All	All

Vendor Declared Affected Products

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wazuh	Wazuh GitHub Actions	affected 4.12.0 semver	Not specified

References

Reference	Source	Link
www.vulncheck.com/advisories/exposure-of-the-github-token-in-wazuh-workflow-run...	disclosure@vulncheck.com	www.vul
github.com/wazuh/wazuh/security/advisories/GHSA-6xqr-4q5g-xc7x	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.c
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: jackhac (en)

CNA: nopcorn (en)

CNA: nopcorn (en)

CNA: vikman90 (en)

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