Wazuh Provisioning Scripts / Build Infrastructure Improper Certificate Validation leading to MITM and RCE

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-15612
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-27 19:16:41 UTC
Updated	2026-03-30 13:26:29 UTC
Description	Wazuh provisioning scripts and Dockerfiles contain an insecure transport vulnerability where curl is invoked with the -k/--ins

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/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: 0.000420000 probability, percentile 0.128510000 (date 2026-04-01)

Problem Types: CWE-295 | CWE-829 | CWE-295 CWE-295 Improper Certificate Validation | CWE-829 CWE-829: Inclusion of Functionality from Untrusted Control Sphere

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Wazuh	Wazuh Provisioning Scripts Agent Build Environment	affected >=4.1.3 semver	Not specified

CNA	Wazuh	Wazuh Provisioning Scripts Agent Build Environment	unaffected >=4.14.0 semver	Not specified

References

Reference	Source	Link	Tag
github.com/wazuh/wazuh/security/advisories/GHSA-wvg9-7q49-c7mg	disclosure@vulncheck.com	github.com	
www.vulncheck.com/advisories/various-uses-of-curl-without-verifying-the-authent...	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

Vendor Comments And Credit

Discovery Credit

CNA: JLLeitschuh (en)

CNA: vikman90 (en)

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