



Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') in coolercontrold

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-5208
State	PUBLISHED
Assigner	GitLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 12:16:22 UTC
Updated	2026-04-16 01:06:47 UTC
Description	Command injection in alerts in CoolerControl/coolercontrold <4.0.0 allows authenticated attackers to execute arbitrary code

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

EPSS: 0.003700000 probability, percentile 0.588640000 (date 2026-04-21)

Problem Types: CWE-78 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	cve@gitlab.com	Secondary	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/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	Coolercontrol	Coolercontrold	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CoolerControl	Coolercontrold	affected 3.1.0 4.0.0 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.com/coolercontrol/coolercontrol/-/releases/4.0.0	cve@gitlab.com	gitlab.com	Release Notes
gitlab.com/coolercontrol/coolercontrol/-/blob/3.1.0/coolercontrold/src/a...	cve@gitlab.com	gitlab.com	Product
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: <https://gitlab.com/lassi-3> (en)

Additional Advisory Data

Solutions

CNA: Upgrade to version 4.0.0

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

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 registered 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