



# Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in coolercontrol-ui

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

## Summary

<b>CVE</b>	CVE-2026-5301
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitLab
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 13:16:43 UTC
<b>Updated</b>	2026-04-16 00:47:16 UTC
<b>Description</b>	Stored XSS in log viewer in CoolerControl/coolercontrol-ui <4.0.0 allows unauthenticated attackers to take over the service

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**EPSS:** 0.000280000 probability, percentile 0.080990000 (date 2026-04-21)

**Problem Types:** CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	cve@gitlab.com	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L
3.1	CNA	CVSS	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### 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	Coolercontrol-ui	affected 2.0.0 4.0.0 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="https://gitlab.com/coolercontrol/coolercontrol/-/releases/4.0.0">gitlab.com/coolercontrol/coolercontrol/-/releases/4.0.0</a>	cve@gitlab.com	<a href="https://gitlab.com">gitlab.com</a>	Release Notes
<a href="https://gitlab.com/coolercontrol/coolercontrol/-/blob/2.0.0/coolercontrol-ui/src...">gitlab.com/coolercontrol/coolercontrol/-/blob/2.0.0/coolercontrol-ui/src...</a>	cve@gitlab.com	<a href="https://gitlab.com">gitlab.com</a>	Product
<a href="https://gitlab.com/coolercontrol/coolercontrol/-/blob/3.1.1/coolercontrol-ui/src...">gitlab.com/coolercontrol/coolercontrol/-/blob/3.1.1/coolercontrol-ui/src...</a>	cve@gitlab.com	<a href="https://gitlab.com">gitlab.com</a>	Product
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)