



# CVE-2025-67298

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

## Summary

<b>CVE</b>	CVE-2025-67298
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-11 15:16:21 UTC
<b>Updated</b>	2026-04-07 01:19:45 UTC
<b>Description</b>	An issue in ClassroomIO before v.0.2.6 allows a remote attacker to escalate privileges via the endpoints /api/verify and /rest

## Risk And Classification

**Primary CVSS:** v3.1 8.1 HIGH from ADP

**CVSS:** [3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**EPSS:** 0.000730000 probability, percentile 0.220170000 (date 2026-04-07)

**Problem Types:** CWE-290 | CWE-345 | CWE-639 | n/a | CWE-345 CWE-345 Insufficient Verification of Data Authenticity | CWE-290 CWE-290 Authentication Bypass by Spoofing | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.1	HIGH	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H</a>
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H</a>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

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	Classroomio	Classroomio	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

### References

Reference	Source	Link	Tags
github.com/classroomio/classroomio/releases/tag/v0.2.6	cve@mitre.org	<a href="#">github.com</a>	Release Notes
gist.github.com/prashunbaral/70c4f6f9d9ff8b82295623073eb41f3a	cve@mitre.org	<a href="#">gist.github.com</a>	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	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 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](#)