CVE-2025-67298

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-67298
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-11 15:16:21 UTC
Updated	2026-04-07 01:19:45 UTC
Description	An issue in ClasroomIO 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	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

ntegrity

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	github.com	Release Notes
gist.github.com/prashunbaral/70c4f6f9d9ff8b82295623073eb41f3a	cve@mitre.org	gist.github.com	Exploit, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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