OpenLearnX has Critical Remote Code Execution Through Python Sandbox Escape via Code Execution Environment

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

Summary

CVE	CVE-2026-41900
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 04:16:18 UTC
Updated	2026-05-08 04:16:18 UTC
Description	OpenLearnX is an open-source, decentralized learning and assessment platform. Prior to version 2.0.3, a remote code exe

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from security-advisories@github.com

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

Problem Types: CWE-78 | CWE-94 | CWE-250 | CWE-284 | CWE-693 | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-250 CWE-250: Execution with Unnecessary Privileges | CWE-284 CWE-284: Improper Access Control | CWE-693 CWE-693: Protection Mechanism Failure

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Th30d4y	OpenLearnX	affected < 2.0.3	Not specified

References

Reference	Source	Link	Ta
github.com/th30d4y/OpenLearnX/commit/14765d7d1856d564747c55c5412e2f38fea...	security-advisories@github.com	github.com	
github.com/th30d4y/OpenLearnX/security/advisories/GHSA-8h25-q488-4hxw	security-advisories@github.com	github.com	
github.com/th30d4y/OpenLearnX/releases/tag/v2.0.3-security-fix	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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