



# Reflected XSS in ATutor

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

## Summary

<b>CVE</b>	CVE-2026-6956
<b>State</b>	PUBLISHED
<b>Assigner</b>	CERT-PL
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-11 10:16:15 UTC
<b>Updated</b>	2026-05-12 14:15:25 UTC
<b>Description</b>	ATutor is vulnerable to Reflected XSS in /install/install.php endpoint. An attacker can provide a specially crafted URL that, v

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from cvd@cert.pl

**CVSS:**4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000770000 probability, percentile 0.227580000 (date 2026-05-12)

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

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/C...
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ATutor	ATutor	affected 2.2.4 semver	Not specified

### References

Reference	Source	Link	Tags
atutor.github.io	cvd@cert.pl	atutor.github.io	
cert.pl/en/posts/2026/05/CVE-2026-6909	cvd@cert.pl	cert.pl	
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:** Michał Majchrowicz (AFINE) (en)

**CNA:** Marcin Wyczechowski (AFINE) (en)

**CNA:** Pawel Zdunek (AFINE) (en)

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

[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)