# Azure Machine Learning Notebook Spoofing Vulnerability

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-32207 |
| **State** | PUBLISHED |
| **Assigner** | microsoft |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-07 22:16:33 UTC |
| **Updated** | 2026-05-08 19:55:25 UTC |
| **Description** | Improper neutralization of input during web page generation ('cross-site scripting') in Azure Machine Learning allows an una |

## 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:** 0.000480000 probability, percentile 0.149150000 (date 2026-05-11)

**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 | secure@microsoft.com | Secondary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C |

## 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 | Microsoft | Azure Machine Learning | - | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Microsoft | Azure Machine Learning | affected - | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32207 | secure@microsoft.com | msrc.microsoft.com | Vendor 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.