# Azure Machine Learning Notebook Spoofing Vulnerability

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-33833 |
| **State** | PUBLISHED |
| **Assigner** | microsoft |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-12 18:17:05 UTC |
| **Updated** | 2026-05-13 15:34:52 UTC |
| **Description** | Improper neutralization of special elements in output used by a downstream component ('injection') in Azure Machine Learr |

## Risk And Classification

**Primary CVSS:** v3.1 8.2 HIGH from secure@microsoft.com

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

**EPSS:** 0.000510000 probability, percentile 0.157980000 (date 2026-05-18)

**Problem Types:** CWE-74 | CWE-74 CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | secure@microsoft.com | Primary | 8.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N |
| 3.1 | CNA | CVSS | 8.2 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N/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

High

ntegrity

Low

Availability

None

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

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Microsoft | Azure Machine Learning | affected 3.0.0 1.7.6 custom | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33833 | secure@microsoft.com | msrc.microsoft.com | |
| 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.