



# After Effects | Out-of-bounds Write (CWE-787)

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

## Summary

|                        |                                                                                                                                   |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2026-34643                                                                                                                    |
| <b>State</b>           | PUBLISHED                                                                                                                         |
| <b>Assigner</b>        | adobe                                                                                                                             |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                      |
| <b>Published</b>       | 2026-05-12 18:17:10 UTC                                                                                                           |
| <b>Updated</b>         | 2026-05-13 19:35:33 UTC                                                                                                           |
| <b>Description</b>     | After Effects versions 26.0, 25.6.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitra |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from psirt@adobe.com

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

**EPSS:** 0.000250000 probability, percentile 0.071480000 (date 2026-05-13)

**Problem Types:** CWE-787 | CWE-787 Out-of-bounds Write (CWE-787)

| Version | Source          | Type    | Score | Severity | Vector                                       |
|---------|-----------------|---------|-------|----------|----------------------------------------------|
| 3.1     | psirt@adobe.com | Primary | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1     | CNA             | CVSS    | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product       | Version | Update | Edition | Language |
|-------------|--------|---------------|---------|--------|---------|----------|
| Application | Adobe  | After Effects | All     | All    | All     | All      |
| Application | Adobe  | After Effects | 26.0    | All    | All     | All      |

Vendor Declared Affected Products

| Source | Vendor | Product       | Version                | Platforms     |
|--------|--------|---------------|------------------------|---------------|
| CNA    | Adobe  | After Effects | affected 25.6.4 semver | Not specified |

References

| Reference                                                      | Source          | Link            | Tags                |
|----------------------------------------------------------------|-----------------|-----------------|---------------------|
| helpx.adobe.com/security/products/after_effects/apsb26-48.html | psirt@adobe.com | helpx.adobe.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.