



# Acrobat Reader | Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (CWE-1321)

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-34622  |
| <b>State</b>           | PUBLISHED   |
| <b>Assigner</b>        | adobe   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2026-04-14 17:16:51 UTC   |
| <b>Updated</b>         | 2026-04-16 14:14:56 UTC   |
| <b>Description</b>     | Acrobat Reader versions 26.001.21411, 24.001.30360, 24.001.30362 and earlier are affected by an Improperly Controlled I |

## Risk And Classification

**Primary CVSS:** v3.1 8.6 HIGH from psirt@adobe.com

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

**EPSS:** 0.002350000 probability, percentile 0.464580000 (date 2026-04-21)

**Problem Types:** CWE-1321 | CWE-1321 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (CWE-1321)

| Version | Source          | Type      | Score | Severity | Vector                                       |
|---------|-----------------|-----------|-------|----------|--|
| 3.1     | psirt@adobe.com | Secondary | 8.6   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H |
| 3.1     | CNA             | CVSS      | 8.6   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

#### NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor    | Product           | Version | Update | Edition | Language |
|------------------|-----------|-------------------|---------|--------|---------|----------|
| Application      | Adobe     | Acrobat           | All     | All    | All     | All      |
| Application      | Adobe     | Acrobat Dc        | All     | All    | All     | All      |
| Application      | Adobe     | Acrobat Reader Dc | All     | All    | All     | All      |
| Operating System | Apple     | Macos             | -       | All    | All     | All      |
| Operating System | Microsoft | Windows           | -       | All    | All     | All      |

#### Vendor Declared Affected Products

| Source | Vendor | Product        | Version                      | Platforms     |
|--------|--------|----------------|------------------------------|---------------|
| CNA    | Adobe  | Acrobat Reader | affected 26.001.21411 semver | Not specified |

#### References

| Reference  | Source          | Link  | Tags                |
|--|-----------------|---|---------------------|
| helpx.adobe.com/security/products/acrobat/apsb26-44.html | psirt@adobe.com | <a href="https://helpx.adobe.com">helpx.adobe.com</a> | Vendor Advisory     |
| CVE Program record                                       | CVE.ORG         | <a href="https://www.cve.org">www.cve.org</a>         | canonical           |
| NVD vulnerability detail                                 | NVD             | <a href="https://nvd.nist.gov">nvd.nist.gov</a>       | canonical, analysis |

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

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)