



CVE-2021-44704

Published on: Not Yet Published

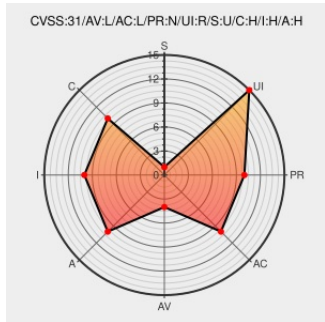
Last Modified on: 01/21/2022 08:33:00 PM UTC

CVE-2021-44704

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Acrobat](#) from [Adobe](#) contain the following vulnerability:

Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by a use-after-free vulnerability in the processing of Format event actions that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE-2021-44704 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 21.007.20099

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 20.004.30017

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 17.011.30204

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= None

CVSS3 Score: **7.8 - HIGH**

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---------------|------------------------|---------------------|---------------------|
| LOCAL | LOW | NONE | REQUIRED |
| Scope | Confidentiality Impact | Integrity Impact | Availability Impact |
| UNCHANGED | HIGH | HIGH | HIGH |

CVSS2 Score: **9.3 - HIGH**


| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | MEDIUM | NONE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| | | |

COMPLETE

COMPLETE

COMPLETE

CVE References

| Description | Tags | Link |
|-------------------------|---|--|
| Adobe Security Bulletin | helpx.adobe.com text/html |  MISC helpx.adobe.com/security/products/acrobat/apsb22-01.html |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

376233 Adobe Security Update for Adobe Acrobat and Adobe Reader (APSB22-01)

Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-----------|-------------------|---------|--------|---------|----------|
| Application | Adobe | Acrobat | All | All | All | All |
| Application | Adobe | Acrobat | All | All | All | All |
| Application | Adobe | Acrobat Dc | All | All | All | All |
| Application | Adobe | Acrobat Reader | All | All | All | All |
| Application | Adobe | Acrobat Reader | 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 |

cpe:2.3:a:adobe:acrobat:*:*:*:classic:*:*:

cpe:2.3:a:adobe:acrobat:*:*:*:classic:*:*:

cpe:2.3:a:adobe:acrobat_dc:*:*:*:continuous:*:*:

cpe:2.3:a:adobe:acrobat_reader:*:*:*:classic:*:*:

cpe:2.3:a:adobe:acrobat_reader:*:*:*:classic:*:*:




cpe:2.3:a:adobe:acrobat_reader_dc:*:*:*:continuous:*:*:

cpe:2.3:o:apple:macos:-:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|--|--|------------------------|
|  @CVereport | CVE-2021-44704 : Acrobat Reader DC version 21.007.20099 and earlier , 20.004.30017 and earlier and 17.011.30204... twitter.com/i/web/status/1... | 2022-01-14 20:16:12 |
|  /r/k12cybersecurity | MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Adobe Products Could Allow for Arbitrary Code Execution - PATCH: NOW | 2022-01-12 14:16:08 |
|  /r/netcve | CVE-2021-44704 | 2022-01-14 20:38:52 |

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2022   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report