



CVE-2021-21042

Published on: 02/11/2021 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:29:00 AM UTC

CVE-2021-21042

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



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

Acrobat Reader DC versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Read vulnerability that could lead to arbitrary disclosure of information in the memory stack. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.

Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE-2021-21042 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 2020.013.20074

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 2020.001.30018

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 2017.011.30188

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

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Adobe Security Bulletin	Vendor Advisory helpx.adobe.com text/html	 MISC helpx.adobe.com/security/products/acrobat/apsb21-09.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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Exploit code for CVE-2021-21042

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	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	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:apple:mac_os:-:~::~:~::~:
cpe:2.3:o:apple:mac_os:-:~::~:~::~:
cpe:2.3:o:apple:mac_os:-:~::~:~::~:
cpe:2.3:o:microsoft:windows:-:~::~:~::~:
cpe:2.3:o:microsoft:windows:-:~::~:~::~:
cpe:2.3:o:microsoft:windows:-:~::~:~::~:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @j00sean	1) CVE-2021-21042 to disclosure user32.dll's base addr. 2) CVE-2019-7040 to get RCE. No sbx, so protected mode is... twitter.com/i/web/status/1...	2022-06-29 18:23:23
 @ipssignatures	CheckPoint has a protection/signature/rule for the vulnerability CVE-2021-21042 since about 505 days ago.... twitter.com/i/web/status/1...	2022-06-29 22:04:02
 @ipssignatures	Hillstone has a protection/signature/rule for the vulnerability CVE-2021-21042 since about 246 days ago.... twitter.com/i/web/status/1...	2022-06-29 22:04:02
 @ipssignatures	WatchGuard has a protection/signature/rule for the vulnerability CVE-2021-21042 since about 379 days ago.... twitter.com/i/web/status/1...	2022-06-29 22:04:02
 @ipssignatures	The vuln CVE-2021-21042 has a tweet created 0 days ago and retweeted 8 times. twitter.com/j00sean/status... #S5qhijdrsnfeo	2022-06-29 22:04:03
 @ipssignatures	The vuln CVE-2021-21042 has a tweet created 0 days ago and retweeted 11 times. twitter.com/j00sean/status... #pow1rtrtwwcve	2022-06-30 00:06:01
 @j00sean	Full disclosure for CVE-2021-21042 + CVE-2019-7040 is ready right here. github.com/j00sean/SecBug...	2022-07-04 19:08:37
 @ipssignatures	The vuln CVE-2021-21042 has a tweet created 0 days ago and retweeted 19 times. twitter.com/j00sean/status... #pow1rtrtwwcve	2022-07-04 22:06:00

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](#)