

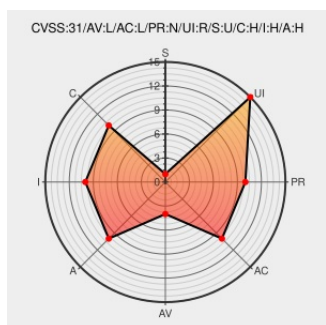


CVE-2020-24435

Published on: 11/05/2020 12:00:00 AM UTC

Last Modified on: 09/08/2021 05:22:00 PM UTC

CVE-2020-24435

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

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

Acrobat Reader DC versions 2020.012.20048 (and earlier), 2020.001.30005 (and earlier) and 2017.011.30175 (and earlier) are affected by a heap-based buffer overflow vulnerability in the submitForm function, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted .pdf file in Acrobat Reader.

CVE-2020-24435 has been assigned by psirt@adobe.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 2017.011.30175

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 2020.012.20048

Affected Vendor/Software: **Adobe - Acrobat Reader** version <= 2020.001.30005

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: **6.8 - MEDIUM**

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

PARTIAL

PARTIAL

PARTIAL

CVE References

Description	Tags	Link
Adobe Security Bulletin	Vendor Advisory helpx.adobe.com text/html	 MISC helpx.adobe.com/security/products/acrobat/apsb20-67.html
TALOS-2020-1157 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory www.talosintelligence.com text/html	 MISC www.talosintelligence.com/vulnerability_reports/TALOS-2020-1157

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

Known Affected Configurations (CPE V2.3)

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 Dc	All	All	All	All
Application	Adobe	Acrobat Reader	All	All	All	All
Application	Adobe	Acrobat Reader Dc	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	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_dc:*.***:classic:***:

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

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

cpe:2.3:a:adobe:acrobat_reader_dc:*.***: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:microsoft:windows:~::~:~::~:
cpe:2.3:o:microsoft:windows:~::~:~::~:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2020-24435.... twitter.com/i/web/status/1...	2021-04-25 09:02:02
 @ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-24435. ipssignatures.appspot.com/?cve=CVE-2020-... #S3rtsnd65g5k4y	2021-04-25 09:02:02
← Previous ID		Next ID →