



# CVE-2022-24960

Published on: Not Yet Published

Last Modified on: 03/17/2022 07:33:00 PM UTC

## CVE-2022-24960

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:31/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:L



Certain versions of **Macos** from **Apple** contain the following vulnerability:

A use after free vulnerability was discovered in PDFTron SDK version 9.2.0. A crafted PDF can overwrite RIP with data previously allocated on the heap. This issue affects: PDFTron PDFTron SDK 9.2.0 on OSX; 9.2.0 on Linux; 9.2.0 on Windows.

CVE-2022-24960 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

### Vulnerability Patch/Work Around

No known workarounds exist.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>LOCAL</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>NONE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

### CVE References

Description	Tags	Link
-------------	------	------

PDFTron Systems Inc. | Nightly

[www.pdftron.com](http://www.pdftron.com)  
text/html

MISC [www.pdftron.com/nightly/#stable/2022-02-08/9.2/](http://www.pdftron.com/nightly/#stable/2022-02-08/9.2/)

security\_research/CVE-2022-24960.json at main · suletm/security\_research · GitHub

[github.com](https://github.com)  
text/html

MISC [github.com/suletm/security\\_research/blob/main/CVE/CVE-2022-24960.json](https://github.com/suletm/security_research/blob/main/CVE/CVE-2022-24960.json)

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](mailto: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
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	-	All	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	-	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All
Application	<a href="#">Pdftron</a>	<a href="#">Pdftron</a>	9.2.0	All	All	All

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

cpe:2.3:a:linux:linux\_kernel:-:\*:\*:\*:\*:\*:

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

cpe:2.3:a:pdftron:pdftron:9.2.0:\*:\*:\*:\*:\*:

### Discovery Credit

Alex Niu, Tofig Suleymanov

### Social Mentions

Source	Title	Posted (UTC)
<a href="#">@CVEreport</a>	<a href="https://cve.report/CVE-2022-24960">cve.report/CVE-2022-24960</a> A use after free vulnerability was discovered in PDFTron SDK version 9.2.0. A crafted PDF... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-03-10 19:42:37

[← 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](#)**