



CVE-2022-28681

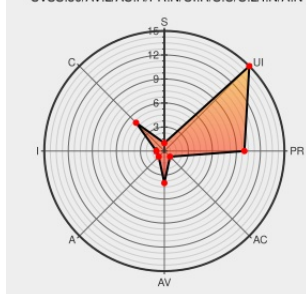
Published on: Not Yet Published

Last Modified on: 08/25/2022 08:10:00 PM UTC

CVE-2022-28681

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

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



Certain versions of [Pdf Editor](#) from [Foxit](#) contain the following vulnerability:

This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.2.1.53537. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deletePages method. By performing actions in

JavaScript, an attacker can trigger a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16825.

CVE-2022-28681 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Foxit - PDF Reader** version **11.2.1.53537**

CVSS3 Score: **6.1 - MEDIUM**

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

CVE References

Description	Tags	Link
Security Bulletins Foxit	www.foxit.com text/html	MISC www.foxit.com/support/security-bulletins.html
ZDI-22-772 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-22-772/

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

376763 Foxit Reader and Foxit PDF Editor Prior to 11.2.2 Multiple Security Vulnerabilities

376801 Foxit PhantomPDF Prior to 10.1.8 Multiple Security Vulnerabilities

Exploit/POC from Github

This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF R...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Foxit	Pdf Editor	All	All	All	All
Application	Foxit	Pdf Editor	All	All	All	All
Application	Foxit	Pdf Reader	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
cpe:2.3:a:foxit:pdf_editor:*:*:*:*:*:						
cpe:2.3:a:foxit:pdf_editor:*:*:*:*:*:						
cpe:2.3:a:foxit:pdf_reader:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows:-:*:*:*:*:						

Discovery Credit

Anonymous

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-28681 : This vulnerability allows remote attackers to disclose sensitive information on affected installat... twitter.com/i/web/status/1...	2022-07-18 18:55:07
 /r/netcve	CVE-2022-28681	2022-07-18 19:39:11

[← Previous ID](#)

Next ID→

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](#)