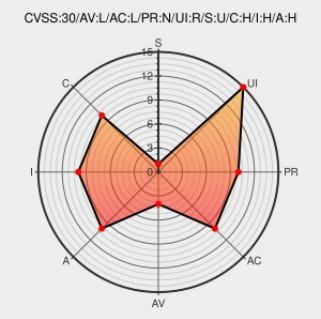
CVE-2021-31476

Published on: 06/16/2021 12:00:00 AM UTC

Last Modified on: 06/29/2021 03:09:05 PM UTC

CVE-2021-31476

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Foxit Reader from Foxitsoftware contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.3.37598. 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 handling of XFA templates. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13531.

CVE-2021-31476 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Foxit** - **PhantomPDF** version **10.1.3.37598**

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
Security Bulletins | Foxit	www.foxit.com text/html	MISC www.foxit.com/support/security-bulletins.html
ZDI-21-614 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-614/

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	Foxitsoftware	Foxit Reader	All	All	All	All
Application	Foxitsoftware	Phantompdf	All	All	All	All
Application	Foxitsoftware	Phantompdf	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:foxitsoftware:foxit_reader:*:*:*:*:*:*:*:*:

cpe:2.3:a:foxitsoftware:phantompdf:*:*:*:*:*:*:*:*:

cpe:2.3:a:foxitsoftware:phantompdf:*:*:*:*:*:*:*:*:

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

Discovery Credit

cece

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31476 : This vulnerability allows remote attackers to execute arbitrary code on affected installations of… twitter.com/i/web/status/1…	2021-06-16 22:16:40
/r/netcve	CVE-2021-31476	2021-06-16 22:41:22

← Previous ID

Next ID→

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