

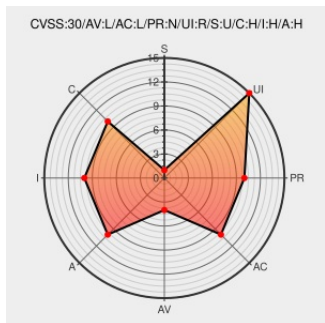


CVE-2020-15638

Published on: 08/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-15638

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

Certain versions of [Phantompdf](#) from [Foxitsoftware](#) contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.2.29539. 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 NodeProperties::InferReceiverMapsUnsafe method. 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-10950.

CVE-2020-15638 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Foxit - PhantomPDF** version **9.7.2.29539**

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
ZDI-20-933 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 MISC www.zerodayinitiative.com/advisories/ZDI-20-933/
Security Bulletins Foxit Software	Vendor Advisory www.foxitsoftware.com text/html	 MISC www.foxitsoftware.com/support/security-bulletins.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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Foxitsoftware	Phantompdf	All	All	All	All
Application	Foxitsoftware	Reader	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
cpe:2.3:a:foxitsoftware:phantompdf:*.*.*.*.*.*.*.*:						
cpe:2.3:a:foxitsoftware:reader:*.*.*.*.*.*.*.*:						
cpe:2.3:o:microsoft:windows:-.*.*.*.*.*.*.*:						
cpe:2.3:o:microsoft:windows:-.*.*.*.*.*.*.*:						

Discovery Credit

Rene Freingruber (@ReneFreingruber) and Patrick Wollgast

[← Previous ID](#)

Next ID→

