



CVE-2018-9947

Published on: 05/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:54 PM UTC

CVE-2018-9947

[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 vulnerable installations of Foxit Reader 9.0.0.29935. 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 parsing of BMP images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, heap-based buffer. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5472.

CVE-2018-9947 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Foxit - Foxit Reader** version **9.0.0.29935**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	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 Software	Patch Vendor Advisory www.foxitsoftware.com text/html	 CONFIRM www.foxitsoftware.com/support/security-bulletins.php
ZDI-18-331 Zero Day Initiative	Third Party Advisory VDB Entry zerodayinitiative.com text/html	 MISC zerodayinitiative.com/advisories/ZDI-18-331

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →