

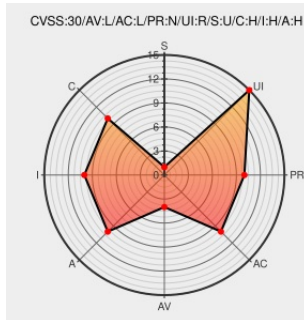


CVE-2020-17416

Published on: 10/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:30 PM UTC

CVE-2020-17416

[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 Reader 10.0.0.35798. 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 JPEG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-11497.

CVE-2020-17416 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Foxit - Reader** version **10.0.0.35798**

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 Software	Vendor Advisory www.foxitsoftware.com text/html	 MISC www.foxitsoftware.com/support/security-bulletins.php
ZDI-20-1233 Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	 N/A N/A

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

376805 Foxit Reader and Foxit PhantomPDF Prior to 10.1 Multiple Security Vulnerabilities

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
Operating System	Microsoft	Windows	-	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:o:microsoft:windows:-:*:*:*:*:
```

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

Discovery Credit

Anonymous

[← Previous ID](#)

Next ID→

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](#)