



# CVE-2018-1177

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

Last Modified on: 03/23/2021 11:24:31 PM UTC

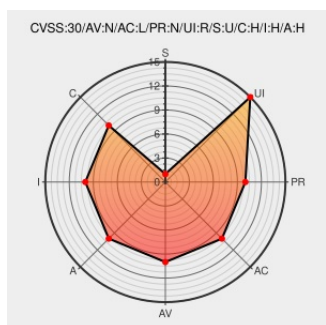
## CVE-2018-1177

[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 handling of the addAnnot method. The issue results from the lack

of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5488.

CVE-2018-1177 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

CVE References

| Description                         | Tags                                                                                                       | Link                                                                                                                                                                                                                     |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Bulletins   Foxit Software | <div>Patch</div> <div>Vendor Advisory</div> <div>www.foxitsoftware.com</div> <div>text/html</div>          |  CONFIRM <a href="http://www.foxitsoftware.com/support/security-bulletins.php">www.foxitsoftware.com/support/security-bulletins.php</a> |
| ZDI-18-315   Zero Day Initiative    | <div>Third Party Advisory</div> <div>VDB Entry</div> <div>zerodayinitiative.com</div> <div>text/html</div> |  MISC <a href="http://zerodayinitiative.com/advisories/ZDI-18-315">zerodayinitiative.com/advisories/ZDI-18-315</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](mailto: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 | <a href="#">Foxitsoftware</a> | <a href="#">Foxit Reader</a> | All     | All    | All     | All      |
| Application | <a href="#">Foxitsoftware</a> | <a href="#">Phantompdf</a>   | 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→