



CVE-2019-5031

Published on: 10/02/2019 12:00:00 AM UTC

Last Modified on: 06/07/2022 06:40:00 PM UTC

CVE-2019-5031

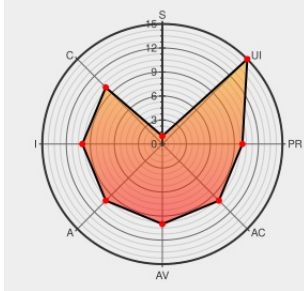
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

An exploitable memory corruption vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader, version 9.4.1.16828. A specially crafted PDF document can trigger an out-of-memory condition which isn't handled properly, resulting in arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this

vulnerability. If the browser plugin extension is enabled, visiting a malicious site can also trigger the vulnerability.

CVE-2019-5031 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

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
TALOS-2019-0702 // Cisco Talos Intelligence Group	CVE-2019-5031	MISC

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Foxitsoftware	Phantompdf	All	All	All	All
Application	Foxitsoftware	Reader	All	All	All	All

```
cpe:2.3:a:foxitsoftware:reader:*.:*:*:*:*:*:
```

Next ID→