



CVE-2018-3959

Published on: 10/02/2018 12:00:00 AM UTC

Last Modified on: 02/02/2023 09:09:00 PM UTC

CVE-2018-3959

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

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

A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader version 9.1.0.5096. A use-after-free condition can occur when accessing the Author property of the this.info object. 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-2018-3959 has been assigned by [cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cisco](#) **Foxit - Foxit PDF Reader** version **Foxit Software Foxit PDF Reader 9.1.0.5096**.

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

Patch

Vendor Advisory

www.foxitsoftware.com

text/html

MISC

www.foxitsoftware.com/support/security-bulletins.php

TALOS-2018-0628 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Third Party Advisory

talosintelligence.com

text/html

MISC

talosintelligence.com/vulnerability_reports/TALOS-2018-0628

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

376808 Foxit PhantomPDF Prior to 8.3.8 Multiple Security Vulnerabilities

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:-:*:*:*:*:						