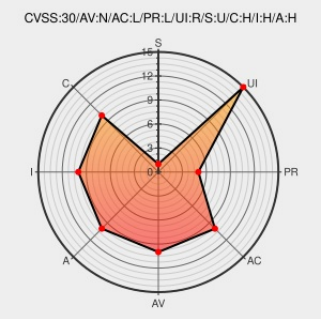
CVE-2019-5130

Published on: 01/16/2020 12:00:00 AM UTC

Last Modified on: 06/14/2022 06:43:00 PM UTC

CVE-2019-5130

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Phantompdf from Foxitsoftware contain the following vulnerability:

An exploitable use-after-free vulnerability exists in the JavaScript engine of Foxit Software's Foxit PDF Reader version 9.7.0.29435. A specially crafted PDF document can trigger a previously freed object in memory to be reused, 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-2019-5130 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-2019-0925 || Cisco Talos Intelligence Group	Exploit	MISC

TALOS-2019-0935 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2019-0935

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	Phantompdf	All	All	All	All
Application	Foxitsoftware	Reader	All	All	All	All

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

cpe:2.3:a:foxitsoftware:reader:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→