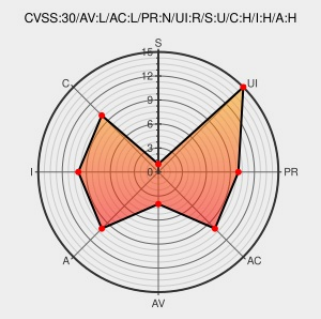
CVE-2018-16297

Published on: 10/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:33 PM UTC

CVE-2018-16297

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 Reader before 9.3 and PhantomPDF before 9.3, a different vulnerability than CVE-2018-16291, CVE-2018-16292, CVE-2018-16293, CVE-2018-16294, CVE-2018-16295, and CVE-2018-16296. 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-2018-16297 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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	CONFIRM www.foxitsoftware.com/support/security-bulletins.php
Foxit Reader Multiple Flaws Let Remote Users Deny Service, Execute Arbitrary Code, and Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041769

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:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→