



# CVE-2018-3850

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-3850
<b>State</b>	PUBLIC
<b>Assigner</b>	talos-cna@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-23 15:29:00 UTC
<b>Updated</b>	2023-01-31 20:15:00 UTC
<b>Description</b>	An exploitable use-after-free vulnerability exists in the JavaScript engine Foxit Software Foxit PDF Reader version 9.0.1.10.

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Foxit</a>	<a href="#">Pdf Reader</a>	9.0.1.1049	All	All	All
Application	<a href="#">Foxitsoftware</a>	<a href="#">Pdf Reader</a>	9.0.1.1049	All	All	All
Application	<a href="#">Foxitsoftware</a>	<a href="#">Pdf Reader</a>	9.0.1.1049	All	All	All

## References

### Reference

- TALOS-2018-0532 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence
- [Foxit Reader Multiple Remote Code Execution Vulnerabilities](#)
- [Foxit Reader Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Obtain Potentially Sensitive Information - SecurityT](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)