



CVE-2017-10952

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

Summary

CVE	CVE-2017-10952
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-29 13:29:00 UTC
Updated	2019-10-09 23:21:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Foxit Reader 8.2.0.2051. L

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Foxitsoftware	Foxit Reader	8.2.0.2051	All	All	All
Application	Foxitsoftware	Foxit Reader	8.2.0.2051	All	All	All

References

Reference

[Zero Day Initiative](#)[Foxit Reader CVE-2017-10952 Remote Code Execution Vulnerability](#)[Foxit Reader File Input Validation Flaw in 'saveAs' JavaScript Function Lets Remote Users Write Files and Execute Arbitrary Code - SecurityT](#)[0patch Blog: 0patching Foxit Reader's saveAs "0day" \(CVE-2017-10952\)](#)[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](#)