



CVE-2017-17557

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

Summary

CVE	CVE-2017-17557
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-24 20:29:00 UTC
Updated	2018-06-05 14:33:00 UTC
Description	In Foxit Reader before 9.1 and Foxit PhantomPDF before 9.1, a flaw exists within the parsing of the BITMAPINFOHEADER

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

[Security Bulletins | Foxit Software](#)

[Opatch Blog: Opatching Foxit Reader Buffer... Oops... Integer Overflow \(CVE-2017-17557\)](#)

[Foxit Reader Multiple Flaws Let Remote Users Execute Arbitrary Code, Deny Service, and Obtain Potentially Sensitive Information - SecurityT](#)

[Foxit Reader and Foxit PhantomPDF CVE-2017-17557 Heap Based Buffer Overflow Vulnerability](#)

[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](#)