



CVE-2017-10994

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

Summary

CVE	CVE-2017-10994
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-07 16:29:00 UTC
Updated	2017-08-24 01:29:00 UTC
Description	Foxit Reader before 8.3.1 and PhantomPDF before 8.3.1 have an Arbitrary Write vulnerability, which allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via crafted PDF documents.

Risk And Classification

Problem Types: CWE-123

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Security Bulletins Foxit Software	CONFIRM	www.foxitsoftware.com
Foxit Reader Multiple Memory Errors Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTrack	www.securitytracker.com
Foxit Reader and Foxit PhantomPDF CVE-2017-10994 Arbitrary Write Remote Code Execution Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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