



CVE-2017-18185

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

Summary

CVE	CVE-2017-18185
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-13 19:29:00 UTC
Updated	2018-05-08 13:29:00 UTC
Description	An issue was discovered in QPDF before 7.0.0. There is a large heap-based out-of-bounds read in the PI_Buffer::write func

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qpdf Project	Qpdf	All	All	All	All
Application	Qpdf Project	Qpdf	All	All	All	All

References

Reference	Source	Link	Tags
USN-3638-1: QPDF vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
Add test case for overflow in PNG filter (fixes #150) · qpdf/qpdf@ec7d74a · GitHub	MISC	github.com	Patch, Third Party Advis
heap out of bounds read (large) in PI_Buffer::write · Issue #150 · qpdf/qpdf · GitHub	MISC	github.com	Issue Tracking, Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

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