CVE-2021-36978

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-36978
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-20 07:15:00 UTC
Updated	2024-01-15 14:15:00 UTC
Description	QPDF 9.x through 9.1.1 and 10.x through 10.0.4 has a heap-based buffer overflow in PI_ASCII85Decoder::write (called fror

Risk And Classification

Problem Types: CWE-787

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	Ta
Heap-use-after-free in `PI_ASCII85Decoder::write` · Issue #492 · qpdf/qpdf · GitHub	MISC	github.com	
Fix some pipelines to be safe if downstream write fails (fuzz issue 2… · qpdf/qpdf@dc92574 · GitHub	MISC	github.com	
QPDF: Buffer Overflow (GLSA 202401-20) — Gentoo security		security.gentoo.org	
oss-fuzz-vulns/OSV-2020-2245.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	github.com	
[SECURITY] [DLA 3548-1] qpdf security update	MLIST	lists.debian.org	
28262 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180596 Debian Security Update for qpdf (CVE-2021-36978)

198446 Ubuntu Security Notification for QPDF vulnerabilities (USN-5026-1)

355553 Amazon Linux Security Advisory for qpdf : ALAS2-2023-2104

6000077 Debian Security Update for qpdf (DLA 3548-1)

710840 Gentoo Linux QPDF Buffer Overflow Vulnerability (GLSA 202401-20)

752442 SUSE Enterprise Linux Security Update for qpdf (SUSE-SU-2022:2669-1)

752443 SUSE Enterprise Linux Security Update for qpdf (SUSE-SU-2022:2670-1)

752576 SUSE Enterprise Linux Security Update for qpdf (SUSE-SU-2022:3248-1)