CVE-2021-32492

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-32492
State	PUBLIC
Assigner	patrick@puiterwijk.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-24 19:15:00 UTC
Updated	2022-03-09 21:39:00 UTC
Description	A flaw was found in djvulibre-3.5.28 and earlier. An out of bounds read in function DJVU::DataPool::has_data() via crafted c

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Djvulibre Project	Djvulibre	All	All	All	All

References

Reference	S
Debian -- Security Information -- DSA-5032-1 djvulibre	D
1943686 – (CVE-2021-32492) CVE-2021-32492 djvulibre: Out of bounds read in function DJVU::DataPool::has_data() via crafted djvu file	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178612 Debian Security Update for djvulibre (DLA 2667-1)

178964 Debian Security Update for djvulibre (DSA 5032-1)

180530 Debian Security Update for djvulibre (CVE-2021-32492)

198375 Ubuntu Security Notification for DjVuLibre vulnerabilities (USN-4957-1)

281495 Fedora Security Update for mingw (FEDORA-2021-f3183da6bb)

281496 Fedora Security Update for mingw (FEDORA-2021-3193a4c13f)

356187 Amazon Linux Security Advisory for djvulibre : ALASMATE-DESKTOP1.X-2023-002

501835 Alpine Linux Security Update for djvulibre

502051 Alpine Linux Security Update for djvulibre

504666 Alpine Linux Security Update for djvulibre

750017 SUSE Enterprise Linux Security Update for djvulibre (SUSE-SU-2021:1649-1)

750022 SUSE Enterprise Linux Security Update for djvulibre (SUSE-SU-2021:1641-1)

750024 SUSE Enterprise Linux Security Update for djvulibre (SUSE-SU-2021:1645-1)

750197 OpenSUSE Security Update for djvulibre (openSUSE-SU-2021:0759-1)

750790 OpenSUSE Security Update for djvulibre (openSUSE-SU-2021:1641-1)