



CVE-2021-3630

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

Summary

CVE	CVE-2021-3630
State	PUBLIC
Assigner	patrick@puiterwijk.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-30 14:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	An out-of-bounds write vulnerability was found in DjVuLibre in DJVU::DjVuTXT::decode() in DjVuText.cpp via a crafted djvu

Risk And Classification

Problem Types: CWE-787

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
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Djvulibre Project	Djvulibre	All	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 33 Update: mingw-djvulibre-3.5.28-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[SECURITY] Fedora 34 Update: djvulibre-3.5.27-30.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[SECURITY] Fedora 33 Update: djvulibre-3.5.27-28.fc33 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 33 Update: mingw-djvulibre-3.5.28-1.fc33 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] Fedora 34 Update: mingw-djvulibre-3.5.28-1.fc34 - package-announce - Fedora Mailing-Lists		lists
[SECURITY] [DLA 2702-1] djvulibre security update	MLIST	lists
[SECURITY] Fedora 34 Update: djvulibre-3.5.27-30.fc34 - package-announce - Fedora Mailing-Lists		lists
Debian -- Security Information -- DSA-5032-1 djvulibre	DEBIAN	www

[SECURITY] Fedora 34 Update: mingw-djvulibre-3.5.28-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists
[SECURITY] Fedora 33 Update: djvulibre-3.5.27-28.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists
1977427 – (CVE-2021-3630) CVE-2021-3630 djvulibre: out-of-bounds write in DJVU::DjVuTXT::decode() in DjVuText.cpp	MISC	bug:
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178694](#) Debian Security Update for djvulibre (DLA 2702-1)

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

[180231](#) Debian Security Update for djvulibre (CVE-2021-3630)

[198427](#) Ubuntu Security Notification for DjVuLibre vulnerability (USN-5005-1)

[281710](#) Fedora Security Update for djvulibre (FEDORA-2021-7514c11a37)

[281711](#) Fedora Security Update for djvulibre (FEDORA-2021-fd6f2727c8)

[281718](#) Fedora Security Update for mingw (FEDORA-2021-d19172badb)

[281719](#) Fedora Security Update for mingw (FEDORA-2021-6422a16aed)

[356165](#) Amazon Linux Security Advisory for djvulibre : ALASMATE-DESKTOP1.X-2023-001

[502051](#) Alpine Linux Security Update for djvulibre

[504666](#) Alpine Linux Security Update for djvulibre

[750918](#) SUSE Enterprise Linux Security Update for djvulibre (SUSE-SU-2021:2621-1)

[750929](#) OpenSUSE Security Update for djvulibre (openSUSE-SU-2021:2619-1)

[750941](#) OpenSUSE Security Update for djvulibre (openSUSE-SU-2021:1112-1)

[750985](#) SUSE Enterprise Linux Security Update for djvulibre (SUSE-SU-2021:2796-1)

© [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](#)