



CVE-2021-33289

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-33289
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-07 14:15:00 UTC
Updated	2023-11-07 03:35:00 UTC
Description	In NTFS-3G versions < 2021.8.22, when a specially crafted MFT section is supplied in an NTFS image a heap buffer overfl

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
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Tuxera	Ntfs-3g	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: ntfs-3g-2021.8.22-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Tuxera – Reliable file systems & storage management software - Tuxera	MISC	ntfs-3g.com
Tuxera – Reliable file systems & storage management software - Tuxera	MISC	tuxera.com
OPEN SOURCE NTFS-3G SECURITY ADVISORY NTFS3G-SA-2021-0001 · Advisory · tuxera/ntfs-3g · GitHub	MISC	github.com
[SECURITY] Fedora 33 Update: ntfs-3g-2021.8.22-2.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
oss-security - NTFS3G-SA-2021-0001: Multiple buffer overflows in all versions of NTFS-3G	MLIST	www.openwall.com/lists/oss-security
[SECURITY] Fedora 35 Update: ntfs-3g-2021.8.22-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Debian -- Security Information -- DSA-4971-1 ntfs-3g	DEBIAN	www.debian.org

[SECURITY] Fedora 33 Update: ntfs-3g-2021.8.22-2.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] [DLA 2819-1] ntfs-3g security update	MLIST	lists.debian.org
NTFS-3G: Multiple Vulnerabilities (GLSA 202301-01) — Gentoo security	GENTOO	security.gentoo.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159858](#) Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-1759)

[178786](#) Debian Security Update for ntfs-3g (DSA 4971-1)

[178900](#) Debian Security Update for ntfs-3g (DLA 2819-1)

[182595](#) Debian Security Update for ntfs-3g (CVE-2021-33289)

[240292](#) Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:1759)

[281928](#) Fedora Security Update for ntfs (FEDORA-2021-e7c8ba6301)

[671164](#) EulerOS Security Update for ntfs-3g (EulerOS-SA-2021-2807)

[710698](#) Gentoo Linux NTFS-3G Multiple Vulnerabilities (GLSA 202301-01)

[751107](#) SUSE Enterprise Linux Security Update for ntfs-3g_ntfsprogs (SUSE-SU-2021:2965-1)

[751113](#) OpenSUSE Security Update for ntfs-3g_ntfsprogs (openSUSE-SU-2021:2971-1)

[751127](#) OpenSUSE Security Update for ntfs-3g_ntfsprogs (openSUSE-SU-2021:1244-1)

[901208](#) Common Base Linux Mariner (CBL-Mariner) Security Update for ntfs-3g (6751-1)

[940525](#) AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2022:1759)

[960314](#) Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:1759)

© [CVE.report](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report