



CVE-2019-11461

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

Summary

CVE	CVE-2019-11461
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-22 21:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	An issue was discovered in GNOME Nautilus 3.30 prior to 3.30.6 and 3.32 prior to 3.32.1. A compromised thumbnailer may

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnome	Nautilus	All	All	All	All
Application	Gnome	Nautilus	All	All	All	All

References

Reference	Source	Link	Tags
(CVE-2019-11461) Incomplete fix for CVE-2017-5226 (#987) · Issues · GNOME / nautilus · GitLab	MISC	gitlab.gnome.org	Issue
Nautilus: Security bypass (GLSA 201908-27) — Gentoo security	GENTOO	security.gentoo.org	
[security-announce] openSUSE-SU-2019:2038-1: moderate: Security update f	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501089](#) Alpine Linux Security Update for nautilus

[671437](#) EulerOS Security Update for nautilus (EulerOS-SA-2022-1356)

[710104](#) CentOS Linux Security Update for nautilus (GLSA 201908-27)

© [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](#).

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