



CVE-2019-13636

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

Summary

CVE	CVE-2019-13636
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-17 21:15:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Patch	All	All	All	All

References

Reference

- patch.git - GNU patch
- [SECURITY] Fedora 30 Update: patch-2.7.6-11.fc30 - package-announce - Fedora Mailing-Lists
- August 2019 GNU patch Vulnerabilities in NetApp Products | NetApp Product Security
- Debian -- Security Information -- DSA-4489-1 patch
- Bugtraq: Details about recent GNU patch vulnerabilities
- [SECURITY] [DLA 1856-1] patch security update
- Bugtraq: [SECURITY] [DSA 4489-1] patch security update
- GitHub - irsl/gnu-patch-vulnerabilities: The GNU patch utility was prone vulnerable to multiple attacks through version 2.7.6. You can find my r
- USN-4071-1: Patch vulnerabilities | Ubuntu security notices
- USN-4071-2: Patch vulnerabilities | Ubuntu security notices | Ubuntu
- [SECURITY] Fedora 30 Update: patch-2.7.6-11.fc30 - package-announce - Fedora Mailing-Lists
- Patch: Multiple vulnerabilities (GLSA 201908-22) — Gentoo security
- GNU patch Command Injection / Directory Traversal ≈ Packet Storm

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296079](#) Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

[377385](#) Alibaba Cloud Linux Security Update for patch (ALINUX3-SA-2022:0056)

[500512](#) Alpine Linux Security Update for patch

[504271](#) Alpine Linux Security Update for patch

[752201](#) SUSE Enterprise Linux Security Update for patch (SUSE-SU-2022:1925-1)

[752207](#) SUSE Enterprise Linux Security Update for patch (SUSE-SU-2022:1932-1)

[900088](#) CBL-Mariner Linux Security Update for patch 2.7.6

[901458](#) Common Base Linux Mariner (CBL-Mariner) Security Update for patch (6789-1)

[903458](#) Common Base Linux Mariner (CBL-Mariner) Security Update for patch (1915)

[940038](#) AlmaLinux Security Update for patch (ALSA-2020:1852)

[960198](#) Rocky Linux Security Update for patch (RLSA-2020:1852)

© [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](#)