



CVE-2021-44731

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

Summary

CVE	CVE-2021-44731
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-17 23:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	A race condition existed in the snapd 2.54.2 snap-confine binary when preparing a private mount namespace for a snap. Th

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canonical	Snapd	All	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	21.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: snapd-2.54.3-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
snap-confine must_mkdir_and_open_with_perms() Race Condition ≈ Packet Storm	MISC	packetstormsecurity
[SECURITY] Fedora 34 Update: snapd-2.54.3-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
USN-5292-1: snapd vulnerabilities Ubuntu security notices Ubuntu	MISC	ubuntu.com
[SECURITY] Fedora 34 Update: snapd-2.54.3-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
Debian -- Security Information -- DSA-5080-1 snapd	DEBIAN	www.debian.org

oss-security - CVE-2021-4120: Insufficient validation of snap content interface and layout paths	MLIST	www.openwall.com
oss-security - Re: CVE-2021-44731: Race condition in snap-confine's setup_private_mount()	MLIST	www.openwall.com
Full Disclosure: Race condition in snap-confine's must_mkdir_and_open_with_perms() (CVE-2022-3328)	FULLDISC	seclists.org
oss-security - Race condition in snap-confine's must_mkdir_and_open_with_perms() (CVE-2022-3328)	MLIST	www.openwall.com
[SECURITY] Fedora 35 Update: snapd-2.54.3-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
oss-security - Re: CVE-2021-44731: Race condition in snap-confine's setup_private_mount()	MLIST	www.openwall.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Qualys Research Team

Legacy QID Mappings

- [179084](#) Debian Security Update for snapd (DSA 5080-1)
- [182283](#) Debian Security Update for snapd (CVE-2021-44731)
- [198668](#) Ubuntu Security Notification for snapd Vulnerabilities (USN-5292-1)
- [198670](#) Ubuntu Security Notification for snapd Vulnerabilities (USN-5292-2)
- [282412](#) Fedora Security Update for snapd (FEDORA-2022-5df8b52ba4)
- [282413](#) Fedora Security Update for snapd (FEDORA-2022-82bea71e5a)
- [376419](#) Snap-Confine Local Privilege Escalation Vulnerability (Oh Snap! More Lemmings)

© [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