



# CVE-2021-3493

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-3493
<b>State</b>	PUBLIC
<b>Assigner</b>	security@ubuntu.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-17 05:15:00 UTC
<b>Updated</b>	2023-07-07 19:10:00 UTC
<b>Description</b>	The overlays implementation in the linux kernel did not properly validate with respect to user namespaces the setting of file

## Risk And Classification

**EPSS:** 0.771920000 probability, percentile 0.989620000 (date 2026-04-01)

**CISA KEV:** Listed on 2022-10-20; due 2022-11-10; ransomware use Unknown

**Problem Types:** CWE-863

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Linux
<b>Product</b>	Kernel
<b>Name</b>	Linux Kernel Privilege Escalation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=7c03e2cda4a584cadc398e8f6641ca9988a39d52">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=7c03e2cda4a584cadc398e8f6641ca9988a39d52</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2021-3493">https://nvd.nist.gov/vuln/detail/CVE-2021-3493</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Ubuntu Overlays Local Privilege Escalation ~ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	
oss-security - [CVE-2021-3493] Ubuntu Linux kernel overlays fs caps privilege escalation	MISC	<a href="https://www.openwall.com">www.openwall.com</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	

<a href="#">kernel/git/torvalds/linux.git - Linux kernel source tree</a>	MISC	<a href="#">git.kernel.org</a>	
<a href="#">Ubuntu OverlayFS Local Privilege Escalation ≈ Packet Storm</a>	MISC	<a href="#">packetstormsecurity.com</a>	
<a href="#">Kernel Live Patch Security Notice LSN-0076-1 ≈ Packet Storm</a>	MISC	<a href="#">packetstormsecurity.com</a>	
<a href="#">USN-4917-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu</a>	MISC	<a href="#">ubuntu.com</a>	
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>	canonica
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>	canonica
<a href="#">CISA Known Exploited Vulnerabilities catalog</a>	CISA	<a href="#">www.cisa.gov</a>	kev

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** An independent security researcher reporting to the SSD Secure Disclosure program

## Legacy QID Mappings

- [180539](#) Debian Security Update for linux (CVE-2021-3493)
- [198331](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4915-1)
- [198332](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4916-1)
- [198333](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4917-1)

© [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](#).

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