



# CVE-2021-3490

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

## Summary

<b>CVE</b>	CVE-2021-3490
<b>State</b>	PUBLIC
<b>Assigner</b>	security@ubuntu.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-04 02:15:00 UTC
<b>Updated</b>	2021-09-14 14:31:00 UTC
<b>Description</b>	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bo

## Risk And Classification

**Problem Types:** CWE-125 | CWE-787

## 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>	20.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	21.04	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.13	rc3	All	All

## References

Reference	Source	Link	Tag
<a href="#">kernel/git/bpf/bpf.git - BPF kernel tree</a>	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="#">USN-4950-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu</a>	UBUNTU	<a href="https://ubuntu.com">ubuntu.com</a>	
<a href="#">USN-4949-1: Linux kernel vulnerabilities   Ubuntu security notices   Ubuntu</a>	UBUNTU	<a href="https://ubuntu.com">ubuntu.com</a>	
<a href="#">June 2021 Linux Kernel 5.12.4 Vulnerabilities in NetApp Products   NetApp Product Security</a>	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
<a href="#">ZDI-21-606   Zero Day Initiative</a>	MISC	<a href="https://www.zerodayinitiative.com">www.zerodayinitiative.com</a>	
<a href="#">Linux eBPF ALU32 32-bit Invalid Bounds Tracking Local Privilege Escalation ≈ Packet Storm</a>	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>	

oss-security - CVE-2021-3490 - Linux kernel eBPF bitwise ops ALU32 bounds tracking	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	can

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Manfred Paul (@\_manfp) of the RedRocket CTF team (@redrocket\_ctf) working with Trend Micro's Zero Day Initiative

## Legacy QID Mappings

<a href="#">180359</a> Debian Security Update for linux (CVE-2021-3490)
<a href="#">198365</a> Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)
<a href="#">198366</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4949-1)
<a href="#">198367</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4950-1)
<a href="#">281159</a> Fedora Security Update for kernel (FEDORA-2021-05152dbcf5)
<a href="#">281160</a> Fedora Security Update for kernel (FEDORA-2021-286375de1e)
<a href="#">353158</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002
<a href="#">353159</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-001
<a href="#">610372</a> Google Pixel Android October 2021 Security Patch Missing
<a href="#">6140185</a> AWS Bottlerocket Security Update for kernel (GHSA-g5jj-9239-qhqc)
<a href="#">750650</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
<a href="#">750652</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
<a href="#">750762</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
<a href="#">750766</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)

© [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](#)