CVE-2021-3489

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3489
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-04 02:15:00 UTC
Updated	2021-09-14 14:30:00 UTC
Description	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel did not check that the allocated size was smaller tha

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.10	All	All	All
Operating System	Canonical	Ubuntu Linux	21.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.13	-	All	All
Operating System	Linux	Linux Kernel	5.13	rc1	All	All
Operating System	Linux	Linux Kernel	5.13	rc2	All	All
Operating System	Linux	Linux Kernel	5.13	rc3	All	All

References

Reference	Source	Link	Tags
USN-4950-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	ubuntu.com	
USN-4949-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	ubuntu.com	
June 2021 Linux Kernel 5.12.4 Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
ZDI-21-590 | Zero Day Initiative	MISC	www.zerodayinitiative.com	
oss-security - CVE-2021-3489 - Linux kernel eBPF RINGBUF map oversized allocation	MLIST	www.openwall.com	
kernel/git/bpf/bpf.git - BPF kernel tree	MISC	git.kernel.org	

CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

LEGACY: Ryota Shiga (@Ga_ryo_) of Flatt Security working with Trend Micro's Zero Day Initiative

Legacy QID Mappings

- 159492 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
- 180029 Debian Security Update for linux (CVE-2021-3489)
- 198365 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)
- 198366 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4949-1)
- 198367 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4950-1)
- 239816 Red Hat Update for kernel security (RHSA-2021:4356)
- 239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
- 281159 Fedora Security Update for kernel (FEDORA-2021-05152dbcf5)
- 281160 Fedora Security Update for kernel (FEDORA-2021-286375de1e)
- 353158 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002
- 353159 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-001
- 610372 Google Pixel Android October 2021 Security Patch Missing
- 6140192 AWS Bottlerocket Security Update for kernel (GHSA-8j78-p9gc-hw4x)
- 750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
- 750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
- 750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
- 750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
- 940265 AlmaLinux Security Update for kernel (ALSA-2021:4356)

CVE.report and Source URL Uptime Status status.cve.report