CVE-2021-3491

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3491
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 14:31:00 UTC
Description	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFER

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

References

Reference	Source	Link
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-21-589 | Zero Day Initiative	MISC	www.zerodayinitiative.
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
oss-security - CVE-2021-3491 - Linux kernel io_uring PROVIDE_BUFFERS MAX_RW_COUNT bypass	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: Billy Jheng Bing-Jhong (@st424204) of STAR Labs working with Trend Micro's Zero Day Initiative

Legacy QID Mappings

179949 Debian Security Update for linux (CVE-2021-3491)

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)

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

610362 Google Pixel Android September 2021 Security Patch Missing

6140097 AWS Bottlerocket Security Update for kernel (GHSA-crg3-8994-x9c3)

750117 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1891-1)

750118 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1890-1)

750121 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1888-1)

750125 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1887-1)

750126 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1889-1)

750139 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1913-1)

750140 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1912-1)

750171 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0843-1)

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)

750741 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0947-1)

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)

750864 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)