Linux Kernel Privilege Escalation Vulnerability

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0847
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-10 17:44:00 UTC
Updated	2024-01-12 16:15:00 UTC
Description	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_pa

Risk And Classification

EPSS: 0.826870000 probability, percentile 0.992300000 (date 2026-04-01)

CISA KEV: Listed on 2022-04-25; due 2022-05-16; ransomware use Unknown

Problem Types: CWE-665

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2022-0847

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Fedoraproject	Fedora	35	All
Operating System	Linux	Linux Kernel	All	All
Hardware	Netapp	H300e	-	All
Operating System	Netapp	H300e Firmware	-	All
Hardware	Netapp	H300s	-	All
Operating System	Netapp	H300s Firmware	-	All
Hardware	Netapp	H410c	-	All
Operating System	Netapp	H410c Firmware	-	All

Hardware	Netapp	H410s	-	All
Operating System	Netapp	H410s Firmware	-	All
Hardware	Netapp	H500e	-	All
Operating System	Netapp	H500e Firmware	-	All
Hardware	Netapp	H500s	-	All
Operating System	Netapp	H500s Firmware	-	All
Hardware	Netapp	H700e	-	All
Operating System	Netapp	H700e Firmware	-	All
Hardware	Netapp	H700s	-	All
Operating System	Netapp	H700s Firmware	-	All
Application	Ovirt	Ovirt-engine	4.4.10.2	All
Application	Redhat	Codeready Linux Builder	-	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All
Operating System	Redhat	Enterprise Linux Eus	8.2	All
Operating System	Redhat	Enterprise Linux Eus	8.4	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.2	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.4	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.2	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.4	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.2	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	8.4	All
Operating System	Redhat	Enterprise Linux For Real Time	8	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv	8	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.2	All
Operating System	Redhat	Enterprise Linux For Real Time For Nfv Tus	8.4	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.2	All
Operating System	Redhat	Enterprise Linux For Real Time Tus	8.4	All
Operating System	Redhat	Enterprise Linux Server Aus	8.2	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All

Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.1	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.2	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	8.4	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.1	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.2	All
Operating System	Redhat	Enterprise Linux Server Update Services For Sap Solutions	8.4	All
Application	Redhat	Virtualization Host	4.0	All
Hardware	Siemens	Scalance Lpe9403	-	All
Operating System	Siemens	Scalance Lpe9403 Firmware	All	All
Hardware	Sonicwall	Sma1000	-	All
Operating System	Sonicwall	Sma1000 Firmware	All	All

References

Reference	Source	Link
Dirty Pipe Local Privilege Escalation ≈ Packet Storm	MISC	packe
Security Vulnerability: Dirty Pipe attack (CVE-2022-0847) | Support | SUSE	MISC	www.
Linux 4.20 KTLS Read-Only Write ≈ Packet Storm		packe
cert-portal.siemens.com/productcert/pdf/ssa-222547.pdf	CONFIRM	cert-p
CVE-2022-0847 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	secur
The Dirty Pipe Vulnerability — The Dirty Pipe Vulnerability documentation	MISC	dirtyp
Dirty Pipe Linux Privilege Escalation ≈ Packet Storm	MISC	packe
Dirty Pipe SUID Binary Hijack Privilege Escalation ≈ Packet Storm	MISC	packe
Security Advisory	CONFIRM	psirt.g
2060795 – (CVE-2022-0847) CVE-2022-0847 kernel: improper initialization of the "flags" member of the new pipe_buffer	MISC	bugzi
Debian -- Security Information -- DSA-5092-1 linux	MITRE	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n
CISA Known Exploited Vulnerabilities catalog	CISA	www.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159695 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9213)

159698 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9210)

159699 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9212)

159700 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-0825)

159701 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9211)

159727 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9245)

159729 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9244)

159760 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9314)

159763 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9313)

179104 Debian Security Update for linux (DSA 5092-1)

182719 Debian Security Update for linux (CVE-2022-0847)

198694 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5317-1)

198728 Ubuntu Security Notification for Linux kernel (Intel IOTG) Vulnerabilities (USN-5362-1)

240125 Red Hat Update for kernel-rt (RHSA-2022:0821)

240128 Red Hat Update for kernel security (RHSA-2022:0825)

240129 Red Hat Update for kernel security (RHSA-2022:0820)

240130 Red Hat Update for kernel-rt (RHSA-2022:0819)

240137 Red Hat Update for kernel-rt (RHSA-2022:0822)

240139 Red Hat Update for kernel (RHSA-2022:0831)

353184 Amazon Linux Security Advisory for kernel : ALAS-2022-1571

353189 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-023

353190 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-011

353195 Amazon Linux Security Advisory for kernel : ALAS2-2022-1761

354279 Amazon Linux Security Advisory for kernel : ALAS2022-2022-039

354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185

354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185

354642 Amazon Linux Security Advisory for kernel : ALAC2012-2022-039

354643 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-040

354644 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-041

355100 Amazon Linux Security Advisory for kernel : ALAS2022-2022-070

355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070

376451 Linux Kernel Local Privilege Escalation Vulnerability (DirtyPipe)

376532 Docker Desktop Multiple Vulnerabilities

376895 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0015)

376910 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0016)

376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)

377053 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0028)

590976 Siemens SCALANCE LPE9403 Third-Party Multiple Vulnerabilities (ICSA-22-167-09) (SSA-222547)

610409 Google Android April 2022 Security Patch Missing for Samsung

610413 Google Android Devices May 2022 Security Patch Missing

610419 Google Android June 2022 Security Patch Missing for Samsung

610420 Google Android June 2022 Security Patch Missing for Huawei EMUI

6140094 AWS Bottlerocket Security Update for kernel (GHSA-jfg3-hf8x-7hm8)

671726 EulerOS Security Update for kernel (EulerOS-SA-2022-1782)

671727 EulerOS Security Update for kernel (EulerOS-SA-2022-1781)

751833 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0757-1)

751836 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0759-1)

751852 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0755-1)

751853 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0760-1)

751999 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0760-1)

753086 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0755-1)

901886 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8900-1)

906340 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8900-2)

940463 AlmaLinux Security Update for kernel (ALSA-2022:0825)

960113 Rocky Linux Security Update for kernel-rt (RLSA-2022:819)

960116 Rocky Linux Security Update for kernel (RLSA-2022:825)

960782 Rocky Linux Security Update for kernel-rt (RLSA-2022:0819)

960805 Rocky Linux Security Update for kernel (RLSA-2022:0825)