CVE-2021-37576

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-37576
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-26 22:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
oss-security - Re: Linux kernel: powerpc: KVM guest to host memory corruption	MLIST	www.openwall.com
Linux kernel: powerpc: KVM guest to host memory corruption		lore.kernel.org
[SECURITY] Fedora 34 Update: kernel-tools-5.13.6-200.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE-2021-37576 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 34 Update: kernel-tools-5.13.6-200.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Linux kernel: powerpc: KVM guest to host memory corruption	MISC	lore.kernel.org
Debian -- Security Information -- DSA-4978-1 linux	DEBIAN	www.debian.org
[SECURITY] Fedora 33 Update: kernel-tools-5.13.6-100.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 33 Update: kernel-tools-5.13.6-100.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org

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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159379 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-3447)
- 159415 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-3801)
- 178809 Debian Security Update for linux (DSA 4978-1)
- 180159 Debian Security Update for linux (CVE-2021-37576)
- 198514 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5091-1)
- 198515 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-1)
- 198520 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5094-1)
- 198523 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-2)
- 239611 Red Hat Update for kernel (RHSA-2021:3447)
- 239612 Red Hat Update for kernel (RHSA-2021:3446)
- 239614 Red Hat Update for kernel (RHSA-2021:3444)
- 239615 Red Hat Update for kpatch-patch (RHSA-2021:3443)
- 239616 Red Hat Update for kpatch-patch (RHSA-2021:3442)
- 239621 Red Hat Update for kpatch-patch (RHSA-2021:3436)
- 239663 Red Hat Update for kpatch-patch (RHSA-2021:3768)
- 239676 Red Hat Update for kernel (RHSA-2021:3801)
- 257119 CentOS Security Update for kernel (CESA-2021:3801)
- 281754 Fedora Security Update for kernel (FEDORA-2021-12618d9b08)
- 281755 Fedora Security Update for kernel (FEDORA-2021-817b3d47d2)
- 352871 Amazon Linux Security Advisory for kernel : ALAS-2021-1539
- 353097 Amazon Linux Security Advisory for kernel : ALAC2012-2021-033
- 353098 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-034
- 353099 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-035
- 670707 EulerOS Security Update for kernel (EulerOS-SA-2021-2465)

671252 EulerOS Security Update for kernel (EulerOS-SA-2022-1171)

750946 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2647-1)

750947 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2644-1)

750949 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1142-1)

750953 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2645-1)

750963 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2687-1)

751036 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 12 SP3) (SUSE-SU-2021:2846-1)

751037 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 12 SP3) (SUSE-SU-2021:2842-1)

751437 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)

751441 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)

751451 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)

751473 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)

751476 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)

900286 CBL-Mariner Linux Security Update for kernel 5.10.52.1

900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1

900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1

901695 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6579-1)

903093 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4894)

906104 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4894-1)

940058 AlmaLinux Security Update for kernel (ALSA-2021:3447)

960048 Rocky Linux Security Update for kernel (RLSA-2021:3447)