CVE-2021-4154

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4154
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-04 23:15:00 UTC
Updated	2023-01-19 15:53:00 UTC
Description	A use-after-free flaw was found in cgroup1_parse_param in kernel/cgroup/cgroup-v1.c in the Linux kernel's cgroup v1 parse

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.14	-	All	All
Operating System	Linux	Linux Kernel	5.14	rc1	All	All
Application	Netapp	Hci Baseboard Management Controller	h300e	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h300s	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h410s	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h500e	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h500s	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h700e	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h700s	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference
kernel/git/torvalds/linux.git - Linux kernel source tree
2034514 – (CVE-2021-4154) CVE-2021-4154 kernel: local privilege escalation by exploiting the fsconfig syscall parameter leads to container b

Security bulletins | Anthos clusters | Google Cloud

CVE-2021-4154 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

179719 Debian Security Update for linux (CVE-2021-4154)

240013 Red Hat Update for kernel-rt (RHSA-2022:0187)

240015 Red Hat Update for kernel security (RHSA-2022:0186)

240024 Red Hat Update for kpatch-patch (RHSA-2022:0231)

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

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

240144 Red Hat Update for kpatch-patch (RHSA-2022:0849)

610417 Google Android Devices June 2022 Security Patch Missing

610422 Google Android July 2022 Security Patch Missing for Huawei EMUI

610423 Google Android July 2022 Security Patch Missing for Samsung

752126 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1687-1)

753118 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP3) (SUSE-SU-2022:0295-1)

753121 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 17 for SLE 15 SP2) (SUSE-SU-2022:0241-1)

753176 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1676-1)

753211 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 11 for SLE 15 SP2) (SUSE-SU-2022:0291-1)

753268 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP2) (SUSE-SU-2022:0254-1)

753292 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP3) (SUSE-SU-2022:0293-1)

753299 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1669-1)

753369 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP2) (SUSE-SU-2022:0292-1)

753385 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 4 for SLE 15 SP3) (SUSE-SU-2022:0257-1)

900647 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8493)

906219 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8493-1)

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

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

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