CVE-2022-0185

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0185
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-11 18:15:00 UTC
Updated	2023-06-26 18:55:00 UTC
Description	A heap-based buffer overflow flaw was found in the way the legacy_parse_param function in the Filesystem Context functic

Risk And Classification

EPSS: 0.018280000 probability, percentile 0.828340000 (date 2026-04-01)

CISA KEV: Listed on 2024-08-21; due 2024-09-11; ransomware use Unknown

Problem Types: CWE-191

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Heap-Based Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. For more information, please see: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=722d94847de2; https://nvd.nist.gov/vuln/detail/CVE-2022-0185

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	All	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All

Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
2040358 – (CVE-2022-0185) CVE-2022-0185 kernel: fs_context: heap overflow in legacy parameter handling	MISC	bugzill
GitHub - Crusaders-of-Rust/CVE-2022-0185: CVE-2022-0185	MISC	github
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.ker
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
Will's Root: CVE-2022-0185 - Winning a $31337 Bounty after Pwning Ubuntu and Escaping Google's KCTF Containers	MISC	www.v
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
oss-security - Linux kernel: Heap buffer overflow in fs_context.c since version 5.1	MISC	www.c
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
CVE-2022-0185 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	securit
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni
CISA Known Exploited Vulnerabilities catalog	CISA	www.c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159599 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-0188)

159617 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2022-9028)

159618 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2022-9029)

159641 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2022-9147)

159642 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2022-9148)

179012 Debian Security Update for linux (DSA 5050-1)

182962 Debian Security Update for linux (CVE-2022-0185)

198638 Ubuntu Security Notification for Linux kernel Vulnerability (USN-5240-1)

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

240010 Red Hat Update for kernel-rt (RHSA-2022:0176)

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

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

240018 Red Hat Update for kernel (RHSA-2022:0188)

240021 Red Hat Update for kpatch-patch (RHSA-2022:0232)

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

282265 Fedora Security Update for kernel (FEDORA-2022-6d4082d590)

282266 Fedora Security Update for kernel (FEDORA-2022-6352c313b7)

353130 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-021

353151 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-009

353188 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-076

354304 Amazon Linux Security Advisory for kernel : ALAS2022-2022-024

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

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

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

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

377124 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0029)

6140031 AWS Bottlerocket Security Update for kernel (GHSA-p292-533m-7qvw)

751654 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0197-1)

751657 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0198-1)

751666 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0169-1)

751993 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0198-1)

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)

753194 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0288-1)

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

753262 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 11 for SLE 15 SP3) (SUSE-SU-2022:0262-1)

753267 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0169-1)

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)

753329 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 19 for SLE 15 SP2) (SUSE-SU-2022:0238-1)

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)

753423 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 15 SP3) (SUSE-SU-2022:0270-1)

753462 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0289-1)

753493 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15 SP2) (SUSE-SU-2022:0239-1)

900672 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8570)

901777 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8578-1)

906211 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8570-1)

906259 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8578-2)

940434 AlmaLinux Security Update for kernel (ALSA-2022:0188)

960076 Rocky Linux Security Update for kernel (RLSA-2022:188)

960100 Rocky Linux Security Update for kernel-rt (RLSA-2022:176)

960786 Rocky Linux Security Update for kernel (RLSA-2022:0188)

960861 Rocky Linux Security Update for kernel-rt (RLSA-2022:0176)

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