CVE-2021-4090

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-4090
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-18 18:15:00 UTC
Updated	2023-11-07 03:40:00 UTC
Description	An out-of-bounds (OOB) memory write flaw was found in the NFSD in the Linux kernel. Missing sanity may lead to a write b

Risk And Classification

Problem Types: CWE-787

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	5.16	-	All	All
Operating System	Linux	Linux Kernel	5.16	rc1	All	All
Hardware	Netapp	Baseboard Management Controller H300e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H300s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410c	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410c Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700e Firmware	-	All	All	All

Hardware	Netapp	Baseboard Management Controller H700s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700s Firmware	-	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
[PATCH v1] NFSD: Fix exposure in nfsd4_decode_bitmap() - Chuck Lever		lore.kernel
CVE-2021-4090 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.ne
[PATCH v1] NFSD: Fix exposure in nfsd4_decode_bitmap() - Chuck Lever	MISC	lore.kernel
2025101 – (CVE-2021-4090) CVE-2021-4090 kernel: Overflow of bmval[bmlen-1] in nfsd4_decode_bitmap function	MISC	bugzilla.re
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

182160 Debian Security Update for linux (CVE-2021-4090)

198624 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5217-1)

198653 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5265-1)

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

136726 Ubuntu Security Notification for Linux kernel (Intel IOTG) Vulnerabilities (USN-5362-1)

900694 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8678)

901154 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8654-1)

906175 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8678-1)

906459 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8654-2)