



# CVE-2021-4090

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-4090
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-18 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:40:00 UTC
<b>Description</b>	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	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.16	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.16	rc1	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700e Firmware</a>	-	All	All	All

Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All

## References

Reference	Source	Link
[PATCH v1] NFSD: Fix exposure in nfsd4_decode_bitmap() - Chuck Lever		<a href="#">lore.kernel</a>
CVE-2021-4090 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.ne</a>
[PATCH v1] NFSD: Fix exposure in nfsd4_decode_bitmap() - Chuck Lever	MISC	<a href="#">lore.kernel</a>
2025101 – (CVE-2021-4090) CVE-2021-4090 kernel: Overflow of bmvval[bmlen-1] in nfsd4_decode_bitmap function	MISC	<a href="#">bugzilla.re</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gc</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">182160</a> Debian Security Update for linux (CVE-2021-4090)
<a href="#">198624</a> Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5217-1)
<a href="#">198653</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5265-1)
<a href="#">198728</a> Ubuntu Security Notification for Linux kernel (Intel IOTG) Vulnerabilities (USN-5362-1)

[100720](#) Ubuntu Security Notification for Linux kernel (Intel CPU) vulnerabilities (CVE-2022-1)

[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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)