



# CVE-2021-3506

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

## Summary

<b>CVE</b>	CVE-2021-3506
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-19 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:38:00 UTC
<b>Description</b>	An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions 1

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
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>	5.12	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.12	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.12	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.12	rc3	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</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
Operating System	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller Firmware</a>	-	All	All	All

## References

Reference	Source
[PATCH] f2fs: fix to avoid out-of-bounds memory access	
CVE-2021-3506 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM
oss-security - Linux kernel: f2fs: out-of-bounds memory access bug	MISC
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST
1944298 – (CVE-2021-3506) CVE-2021-3506 kernel: Out of bounds memory access bug in get_next_net_page() in fs/f2fs/node.c	MISC
[PATCH] f2fs: fix to avoid out-of-bounds memory access	MISC
oss-security - Re: Linux kernel: f2fs: out-of-bounds memory access bug	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">178679</a> Debian Security Update for linux-4.19 (DLA 2690-1)
<a href="#">179603</a> Debian Security Update for linux (CVE-2021-3506)
<a href="#">198416</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4997-1)
<a href="#">198418</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5000-1)
<a href="#">198419</a> Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-5001-1)
<a href="#">198425</a> Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-5000-2)
<a href="#">198426</a> Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-4997-2)
<a href="#">198437</a> Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5016-1) (Sequoia)
<a href="#">198707</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5339-1)
<a href="#">353147</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-004

<a href="#">353158</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002
<a href="#">670514</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2272)
<a href="#">900096</a> CBL-Mariner Linux Security Update for kernel 5.10.52.1
<a href="#">900304</a> CBL-Mariner Linux Security Update for kernel 5.10.57.1
<a href="#">900319</a> CBL-Mariner Linux Security Update for kernel 5.10.60.1
<a href="#">901174</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6571-1)
<a href="#">903011</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4158)
<a href="#">906184</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4158-1)

© [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](#)**