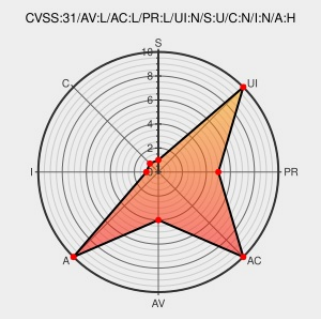
CVE-2021-4148

Published on: Not Yet Published

Last Modified on: 03/30/2022 01:59:00 PM UTC

CVE-2021-4148

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

A vulnerability was found in the Linux kernel's block_invalidatepage in fs/buffer.c in the filesystem. A missing sanity check may allow a local attacker with user privilege to cause a denial of service (DOS) problem.

CVE-2021-4148 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
LKML: Yang Shi: [PATCH] fs: buffer: check huge page size instead of single page for invalidatepage	lkml.org, text/xml	MISC lkml.org/lkml/2021/9/17/1037
LKML: Hao Sun: general protection fault in wb_timer_fn	lkml.org, text/xml	MISC lkml.org/lkml/2021/9/12/323

2026487 – (CVE-2021-4148) CVE-2021-4148 kernel: Improper implementation of block_invalidatepage() allows users to crash the kernel	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2026487

Related QID Numbers

180391 Debian Security Update for linux (CVE-2021-4148)

900779 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9135)

901348 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9135-1)

906220 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9135-2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-4148 : A vulnerability was found in the #Linux #kernel's block_invalidatepage in fs/buffer.c in the filesy… twitter.com/i/web/status/1…	2022-03-23 20:16:15

← Previous ID

Next ID→