



CVE-2018-1000028

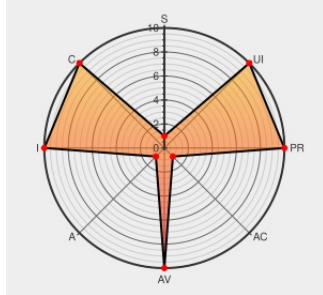
Published on: 02/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000028

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

Linux kernel version after commit bdcf0a423ea1 - 4.15-rc4+, 4.14.8+, 4.9.76+, 4.4.111+ contains a Incorrect Access Control vulnerability in NFS server (nfsd) that can result in remote users reading or writing files they should not be able to via NFS. This attack appear to be exploitable via NFS server must export a filesystem with the

"rootsquash" options enabled. This vulnerability appears to have been fixed in after commit 1995266727fa.

CVE-2018-1000028 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.4 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel	CVE	CONFIRM

kernel/git/torvalds/linux.git - Linux kernel
source tree

Patch

Vendor Advisory

git.kernel.org

text/html

CONFIRM

git.kernel.org/linus/1995266727fa8143897e89b55f5d3c79aa828420

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	4.15	rc4	All	All
Operating System	Linux	Linux Kernel	4.15	rc4	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:4.15:rc4:*****:						
cpe:2.3:o:linux:linux_kernel:4.15:rc4:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)