



CVE-2019-15920

Published on: 09/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15920

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

An issue was discovered in the Linux kernel before 5.0.10. SMB2_read in fs/cifs/smb2pdu.c has a use-after-free. NOTE: this was not fixed correctly in 5.0.10; see the 5.0.11 ChangeLog, which documents a memory leak.

CVE-2019-15920 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
cifs: Fix use-after-free in SMB2_read · torvalds/linux@088aaf1 · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/088aaf17aa79300cab14dbec2569c58cfaf7d6e

September 2019 Linux Kernel
Vulnerabilities in NetApp Products
| NetApp Product Security

Third Party Advisory
security.netapp.com
text/html

 CONFIRM security.netapp.com/advisory/ntap-20191004-0001/

Mailing List

Vendor Advisory

cdn.kernel.org

text/plain

 MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.0.10

[security-announce] openSUSE-
SU-2019:2181-1: important:
Security update

Third Party Advisory
lists.opensuse.org
text/html

 SUSE [openSUSE-SU-2019:2181](https://lists.opensuse.org/2019/09/20/201909200100.html)

[security-announce] openSUSE-
SU-2019:2173-1: important:
Security update

Third Party Advisory
lists.opensuse.org
text/html

 SUSE [openSUSE-SU-2019:2173](https://lists.opensuse.org/2019/09/20/201909200100.html)

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	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:opensuse:leap:15.0:*****:						
cpe:2.3:o:opensuse:leap:15.1:*****:						
cpe:2.3:o:opensuse:leap:15.0:*****:						
cpe:2.3:o:opensuse:leap:15.1:*****:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)