



CVE-2018-1066

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

Summary

CVE	CVE-2018-1066
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-02 08:29:00 UTC
Updated	2019-04-23 13:37:00 UTC
Description	The Linux kernel before version 4.11 is vulnerable to a NULL pointer dereference in fs/cifs/cifsencrypt.c:setup_ntlmv2_rsp()

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
Debian -- Security Information -- DSA-4188-1 linux
kernel/git/torvalds/linux.git - Linux kernel source tree
[SECURITY] [DLA 1422-1] linux security update
USN-3880-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu
[SECURITY] [DLA 1422-2] linux security update

USN-3880-2: Linux kernel (Trusty HWE) vulnerabilities Ubuntu security notices
[stable] cifs: empty TargetInfo leads to crash on recovery - Patchwork
Debian -- Security Information -- DSA-4187-1 linux
CIFS: Enable encryption during session setup phase · torvalds/linux@cabfb36 · GitHub
1539599 – (CVE-2018-1066) CVE-2018-1066 kernel: Null pointer dereference in fs/cifs/cifsencrypt.c:setup_ntlmv2_rsp() when empty TargetIn
Linux Kernel 'fs/cifs/cifsencrypt.c' Denial of Service Vulnerability
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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