

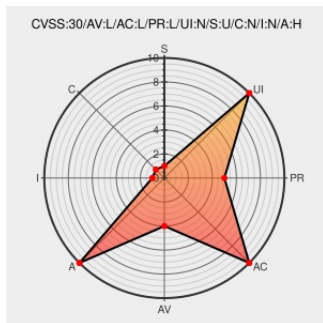


CVE-2019-10140

Published on: 08/15/2019 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:32:00 PM UTC

CVE-2019-10140

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

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

A vulnerability was found in Linux kernel's, versions up to 3.10, implementation of overlays. An attacker with local access can create a denial of service situation via NULL pointer dereference in `ovl_posix_acl_create` function in `fs/overlays/dir.c`. This can allow attackers with ability to create directories on overlays to crash the kernel creating a denial of service (DOS).

CVE-2019-10140 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **OpenSource** - **kernel**: version = up to kernel-3.10

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
-------------	------	------

1677778 – (CVE-2019-10140) CVE-2019-10140 kernel: overlaysfs: NULL pointer dereference in ovl_posix_acl_create function in fs/overlaysfs/dir.c	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1677778
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2019:2043
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2019-10140
1677778 – (CVE-2019-10140) CVE-2019-10140 kernel: overlaysfs: NULL pointer dereference in ovl_posix_acl_create function in fs/overlaysfs/dir.c	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10140
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2019:2029
August 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190905-0002/

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	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)