



CVE-2018-18559

Published on: 10/22/2018 12:00:00 AM UTC

Last Modified on: 05/16/2023 11:14:00 AM UTC

CVE-2018-18559

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H



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

In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between `fanout_add` from `setsockopt` and `bind` on an `AF_PACKET` socket. This issue exists because of the `15fe076edea787807a7cdc168df832544b58eba6` incomplete fix for a race condition. The code mishandles a certain multithreaded case

involving a `packet_do_bind` unregister action followed by a `packet_notifier` register action. Later, `packet_release` operates on only one of the two applicable linked lists. The attacker can achieve Program Counter control.

CVE-2018-18559 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2020:0174
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2019:0188
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:1190
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:4159
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:1170
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHBA-2019:0327
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2019:0163
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:3967
401 Authorization Required	Exploit Patch Third Party Advisory blogs.securiteam.com text/html Inactive Link Not Archived	 MISC blogs.securiteam.com/index.php/archives/3731

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	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
cpe:2.3:o:linux:linux_kernel:*****:*						
cpe:2.3:o:linux:linux_kernel:*****:*						
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*****:*						
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*****:*						
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*****:*						
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*****:*						
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*****:*						
cpe:2.3:a:redhat:openshift_container_platform:3.11:*****:*						
cpe:2.3:a:redhat:openshift_container_platform:3.11:*****:*						

cpe:2.3:a:redhat:openshift_container_platform:3.11.0:EL7:rhel:*

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →