



CVE-2016-9755

Published on: 12/28/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:17 PM UTC

CVE-2016-9755

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

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

The netfilter subsystem in the Linux kernel before 4.9 mishandles IPv6 reassembly, which allows local users to cause a denial of service (integer overflow, out-of-bounds write, and GPF) or possibly have unspecified other impact via a crafted application that makes socket, connect, and writev system calls, related to

net/ipv6/netfilter/nf_conntrack_reasm.c and net/ipv6/netfilter/nf_defrag_ipv6_hooks.c.

CVE-2016-9755 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - CVE Request: Linux: net: out-of-bounds due do a	Mailing List www.openwall.com	MLIST [oss-security] 20161201 CVE Request: Linux: net: out-of-bounds due do a signedness issue when defragging ipv6

signedness issue when defragging ipv6	text/html	
Linux Kernel CVE-2016-9755 Out of Bounds Write Security Vulnerability	cve.report (archive) text/html	BID 94626
[PATCH 10/11] netfilter: ipv6: nf_defrag: drop mangled skb on ream error — Netdev	Mailing List Patch www.spinics.net text/html	MLIST [netdev] 20161130 [PATCH 10/11] netfilter: ipv6: nf_defrag: drop mangled skb on ream error
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=9b57da0630c9fd36ed7a20fc0f98dc82cc0777fa
Bug 1400904 – CVE-2016-9755 kernel: netfilter: Out-of-bounds write due to a signedness issue when defragmenting IPv6 packets	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1400904
netfilter: ipv6: nf_defrag: drop mangled skb on ream error · torvalds/linux@9b57da0 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/9b57da0630c9fd36ed7a20fc0f98dc82cc0777fa
Google Groups	groups.google.com text/html	CONFIRM groups.google.com/forum/#!topic/syzkaller/GFbGpX7nTEo

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
cpe:2.3:o:linux:linux_kernel:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© 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](#)