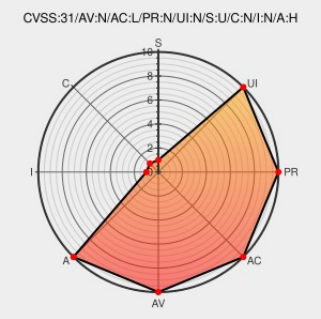
CVE-2016-8666

Published on: 10/16/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:36:00 PM UTC

CVE-2016-8666

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The IP stack in the Linux kernel before 4.6 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for packets with tunnel stacking, as demonstrated by interleaved IPv4 headers and GRE headers, a related issue to CVE-2016-7039.

CVE-2016-8666 has been assigned by security@microfocus.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2047

Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html Inactive Link Not Archived	REDHAT RHSA-2017:0372
Linux Kernel CVE-2016-8666 Stack Overflow Denial of Service Vulnerability	cve.report (archive) text/html	BID 93562
Bug 1384991 – CVE-2016-8666 kernel: Remotely triggerable recursion in GRE code leading to kernel crash	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1384991
tunnels: Don't apply GRO to multiple layers of encapsulation. · torvalds/linux@fac8e0f · GitHub	Issue Tracking Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/fac8e0f579695a3ecbc4d3cac369139d7f819971
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2110
Bug 1001486 – VUL-0: CVE-2016-7039, CVE-2016-8666: kernel-source: remote crash via stack overflow	Issue Tracking Third Party Advisory bugzilla.suse.com text/html	CONFIRM bugzilla.suse.com/show_bug.cgi?id=1001486
oss-security - CVE Request: another recursion in GRE	Mailing List www.openwall.com text/html	MLIST [oss-security] 20161013 CVE Request: another recursion in GRE
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch git.kernel.org text/html	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=fac8e0f579695a3ecbc4d3cac369139d7f819971
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2017:0004
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2107
Broadcom Support Portal	bto.bluecoat.com text/html	CONFIRM bto.bluecoat.com/security-advisory/sa134

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

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

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 registred 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