CVE-2015-5156

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-5156
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-19 10:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	The virtnet_probe function in drivers/net/virtio_net.c in the Linux kernel before 4.2 attempts to support a FRAGLIST feature

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
Linux Kernel Buffer Oveflow in virtio-net GRO Fragmentation Processing Lets Remote Users Cause the Target System to Crash or Potentially
[SECURITY] Fedora 22 Update: kernel-4.2.3-200.fc22
USN-2773-1: Linux kernel vulnerabilities | Ubuntu
Red Hat Customer Portal
[SECURITY] Fedora 21 Update: kernel-4.1.12-101.fc21
USN-2777-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu
Debian -- Security Information -- DSA-3364-1 linux
kernel/git/torvalds/linux.git - Linux kernel source tree
access.redhat.com | CVE-2015-5156
Oracle Linux Bulletin - April 2016
USN-2774-1: Linux kernel (OMAP4) vulnerabilities | Ubuntu

Oracle Linux Bulletin - October 2015
Red Hat Customer Portal
Oracle Linux Bulletin - January 2016
Red Hat Customer Portal
[security-announce] SUSE-SU-2015:1727-1: important: Security update for
Bug 1243852 – CVE-2015-5156 kernel: buffer overflow with fraglist larger than MAX_SKB_FRAGS + 2 in virtio-net
Linux Kernel 'virtio-net' Fragmented Packets Handling Buffer Overflow Vulnerability
[security-announce] SUSE-SU-2015:2292-1: important: Security update for
virtio-net: drop NETIF_F_FRAGLIST · torvalds/linux@48900cb · GitHub
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.