CVE-2016-6835

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

Summary

CVE	CVE-2016-6835
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-10 00:59:00 UTC
Updated	2023-02-12 23:25:00 UTC
Description	The vmxnet_tx_pkt_parse_headers function in hw/net/vmxnet_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest O

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference	Sourc
CVE-2016-6835 - Red Hat Customer Portal	MISC
oss-security - CVE request Qemu: buffer overflow in vmxnet_tx_pkt_parse_headers() in vmxnet3 device emulation	MLIST
[SECURITY] [DLA 1497-1] qemu security update	MLIST
git.qemu.org Git - qemu.git/commit	MISC
git.qemu.org Git - qemu.git/commit	CONF
Bug 1369012 – CVE-2016-6835 Qemu: net: vmxnet: buffer overflow in vmxnet_tx_pkt_parse_headers() in vmxnet3 device emulation	MISC

Red Hat Customer Portal	REDH
oss-security - Re: CVE request Qemu: buffer overflow in vmxnet_tx_pkt_parse_headers() in vmxnet3 device emulation	MLIST
Re: [Qemu-stable] [PATCH] net: vmxnet: check IP header length	MLIST
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.