



CVE-2015-3215

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-3215
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-26 15:29:00 UTC
Updated	2023-02-13 00:48:00 UTC
Description	The NetKVM Windows Virtio driver allows remote attackers to cause a denial of service (guest crash) via a crafted length v

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Virtio-win	-	All	All	All
Application	Redhat	Virtio-win	-	All	All	All

References

Reference	Source
CVE-2015-3215 - Red Hat Customer Portal	MISC
Red Hat Customer Portal	MISC
NetKVM: BZ#1169718: More rigorous testing of incoming packet · YanVugenfirer/kvm-guest-drivers-windows@fbfa4d1 · GitHub	CONFIRM
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	MISC
NetKVM: BZ#1169718: Checking the length only on read · YanVugenfirer/kvm-guest-drivers-windows@723416f · GitHub	CONFIRM
access.redhat.com CVE-2015-3215	MISC
1227634 – (CVE-2015-3215) CVE-2015-3215 virtio-win: netkvm: malformed packet can cause BSOD	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)