



Virtio-win: virtio-win: denial of service via unvalidated descriptor count in unmap request

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

Summary

CVE	CVE-2026-5164
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-30 15:16:36 UTC
Updated	2026-04-01 14:24:21 UTC
Description	A flaw was found in virtio-win. The `RhelDoUnMap()` function does not properly validate the number of descriptors provided

Risk And Classification

Primary CVSS: v3.1 6.7 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000100000 probability, percentile 0.011170000 (date 2026-04-01)

Problem Types: CWE-120 | CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-5164	secalert@redhat.com	access.redhat.com	
github.com/virtio-win/kvm-guest-drivers-windows/pull/1504	secalert@redhat.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
CNA	2026-03-30T14:41:38.036Z	Reported to Red Hat.
CNA	2026-03-30T12:34:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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

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](#)