



# CVE-2009-1565

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

## Summary

<b>CVE</b>	CVE-2009-1565
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT-CNA@flexerasoftware.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-04-12 18:30:00 UTC
<b>Updated</b>	2010-04-22 05:33:00 UTC
<b>Description</b>	vmnc.dll in the VMnc media codec in VMware Movie Decoder before 6.5.4 Build 246459 on Windows, and the movie decod

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Application	Vmware	Movie Decoder	6.5.3	All	All	All
Application	Vmware	Movie Decoder	6.5.3	All	All	All
Application	Vmware	Player	2.5	All	All	All
Application	Vmware	Player	2.5.1	All	All	All
Application	Vmware	Player	2.5.2	All	All	All
Application	Vmware	Player	2.5.3	All	All	All
Application	Vmware	Player	2.5	All	All	All
Application	Vmware	Player	2.5.1	All	All	All
Application	Vmware	Player	2.5.2	All	All	All
Application	Vmware	Player	2.5.3	All	All	All
Application	Vmware	Server	2.0.0	All	All	All
Application	Vmware	Server	2.0.1	All	All	All
Application	Vmware	Server	2.0.2	All	All	All
Application	Vmware	Server	2.0.0	All	All	All
Application	Vmware	Server	2.0.1	All	All	All

Application	<a href="#">Vmware</a>	<a href="#">Server</a>	2.0.2	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.1	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.2	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.3	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.1	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.2	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Workstation</a>	6.5.3	All	All	All

## References

Reference	Source
<a href="#">VMware Server Multiple Vulnerabilities - Advisories - Community</a>	SECUNIA
<a href="#">VMware Products Multiple Vulnerabilities - Advisories - Community</a>	SECUNIA
<a href="#">[Security-announce] VMSA-2010-0007 VMware hosted products, vCenter Server and ESX patches resolve multiple security issues</a>	MLIST
<a href="#">Research - Community</a>	MISC
<a href="#">VMware Workstation Movie Decoder VMnc Multiple Vulnerabilities - Advisories - Community</a>	SECUNIA
<a href="#">NEOHAPSIS - Peace of Mind Through Integrity and Insight</a>	BUGTRAQ
<a href="#">VMware Hosted Products Integer Truncation Multiple Heap Buffer Overflow Vulnerabilities</a>	BID
<a href="#">63615</a>	OSVDB
<a href="#">SecurityTracker.com Archives - VMware Heap Overflows in VMnc Codec Let Remote Users Cause Arbitrary Code to Be Executed</a>	SECTRACKER
<a href="#">VMSA-2010-0007.1</a>	CONFIRMED
<a href="#">NEOHAPSIS - Peace of Mind Through Integrity and Insight</a>	FULLDISCLOSURE
<a href="#">CVE Program record</a>	CVE.OFFICIAL
<a href="#">NVD vulnerability detail</a>	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](#).

