



# CVE-2010-4294

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

## Summary

<b>CVE</b>	CVE-2010-4294
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-12-06 21:05:00 UTC
<b>Updated</b>	2018-10-10 20:08:00 UTC
<b>Description</b>	The frame decompression functionality in the VMnc media codec in VMware Movie Decoder before 6.5.5 build 328052 and

## Risk And Classification

### Problem Types: CWE-94

## 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	6.5.4	All	All	All
Application	Vmware	Movie Decoder	7.0	All	All	All
Application	Vmware	Movie Decoder	7.1.2	All	All	All
Application	Vmware	Movie Decoder	6.5.3	All	All	All
Application	Vmware	Movie Decoder	6.5.4	All	All	All
Application	Vmware	Movie Decoder	7.0	All	All	All
Application	Vmware	Movie Decoder	7.1.2	All	All	All
Application	Vmware	Movie Decoder	All	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	2.5.4	All	All	All
Application	Vmware	Player	2.5.5	All	All	All

Application	Vmware	Player	3.0	All	All	All
Application	Vmware	Player	3.0.1	All	All	All
Application	Vmware	Player	3.1	All	All	All
Application	Vmware	Player	3.1.1	All	All	All
Application	Vmware	Player	3.1.2	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	2.5.4	All	All	All
Application	Vmware	Player	2.5.5	All	All	All
Application	Vmware	Player	3.0	All	All	All
Application	Vmware	Player	3.0.1	All	All	All
Application	Vmware	Player	3.1	All	All	All
Application	Vmware	Player	3.1.1	All	All	All
Application	Vmware	Player	3.1.2	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	Vmware	Server	2.0.2	All	All	All
Application	Vmware	Workstation	6.5.0	All	All	All
Application	Vmware	Workstation	6.5.1	All	All	All
Application	Vmware	Workstation	6.5.2	All	All	All
Application	Vmware	Workstation	6.5.3	All	All	All
Application	Vmware	Workstation	6.5.4	All	All	All
Application	Vmware	Workstation	6.5.5	All	All	All
Application	Vmware	Workstation	7.0	All	All	All
Application	Vmware	Workstation	7.0.1	All	All	All
Application	Vmware	Workstation	7.1	All	All	All
Application	Vmware	Workstation	7.1.1	All	All	All
Application	Vmware	Workstation	7.1.2	All	All	All
Application	Vmware	Workstation	6.5.0	All	All	All
Application	Vmware	Workstation	6.5.1	All	All	All

Application	Vmware	Workstation	6.5.2	All	All	All
Application	Vmware	Workstation	6.5.3	All	All	All
Application	Vmware	Workstation	6.5.4	All	All	All
Application	Vmware	Workstation	6.5.5	All	All	All
Application	Vmware	Workstation	7.0	All	All	All
Application	Vmware	Workstation	7.0.1	All	All	All
Application	Vmware	Workstation	7.1	All	All	All
Application	Vmware	Workstation	7.1.1	All	All	All
Application	Vmware	Workstation	7.1.2	All	All	All

## References

### Reference

SecurityFocus

VMware Movie Decoder VMnc Codec (CVE-2010-4294) Heap Memory Corruption Vulnerability

SecurityTracker.com Archives - VMware Movie Decoder Heap Overflow in Decompression Routine Lets Remote Users Execute Arbitrary Cod

VMware Server Multiple Vulnerabilities - Advisories - Community

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

69596

VMSA-2010-0018

[Security-announce] VMSA-2010-0018 VMware hosted products and ESX patches resolve multiple security issues

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.

© 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](#).

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