



# CVE-2009-2267

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2009-2267
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-11-02 15:30:00 UTC
<b>Updated</b>	2018-10-10 19:39:00 UTC
<b>Description</b>	VMware Workstation 6.5.x before 6.5.3 build 185404, VMware Player 2.5.x before 2.5.3 build 185404, VMware ACE 2.5.x b

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Vmware</a>	<a href="#">Ace</a>	2.5.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Ace</a>	2.5.1	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Ace</a>	2.5.2	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Ace</a>	2.5.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Ace</a>	2.5.1	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Ace</a>	2.5.2	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	2.5.5	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	3.0.3	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	3.5	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	4.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	2.5.5	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	3.0.3	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	3.5	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esx</a>	4.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esxi</a>	3.5	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esxi</a>	4.0	All	All	All
Application	<a href="#">Vmware</a>	<a href="#">Esxi</a>	3.5	All	All	All

Application	Vmware	Esxi	4.0	All	All	All
Application	Vmware	Fusion	2.0	All	All	All
Application	Vmware	Fusion	2.0.1	All	All	All
Application	Vmware	Fusion	2.0.2	All	All	All
Application	Vmware	Fusion	2.0.3	All	All	All
Application	Vmware	Fusion	2.0.4	All	All	All
Application	Vmware	Fusion	2.0.5	All	All	All
Application	Vmware	Fusion	2.0	All	All	All
Application	Vmware	Fusion	2.0.1	All	All	All
Application	Vmware	Fusion	2.0.2	All	All	All
Application	Vmware	Fusion	2.0.3	All	All	All
Application	Vmware	Fusion	2.0.4	All	All	All
Application	Vmware	Fusion	2.0.5	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	All	All	All
Application	Vmware	Player	2.5.1	All	All	All
Application	Vmware	Player	2.5.2	All	All	All
Application	Vmware	Server	1.0	All	All	All
Application	Vmware	Server	1.0.1	All	All	All
Application	Vmware	Server	1.0.2	All	All	All
Application	Vmware	Server	1.0.3	All	All	All
Application	Vmware	Server	1.0.4	All	All	All
Application	Vmware	Server	1.0.5	All	All	All
Application	Vmware	Server	1.0.6	All	All	All
Application	Vmware	Server	1.0.7	All	All	All
Application	Vmware	Server	1.0.8	All	All	All
Application	Vmware	Server	1.0.9	All	All	All
Application	Vmware	Server	2.0	All	All	All
Application	Vmware	Server	2.0	rc2	All	All
Application	Vmware	Server	2.0.1	All	All	All
Application	Vmware	Server	1.0	All	All	All
Application	Vmware	Server	1.0.1	All	All	All
Application	Vmware	Server	1.0.2	All	All	All

Application	Vmware	Server	1.0.3	All	All	All
Application	Vmware	Server	1.0.4	All	All	All
Application	Vmware	Server	1.0.5	All	All	All
Application	Vmware	Server	1.0.6	All	All	All
Application	Vmware	Server	1.0.7	All	All	All
Application	Vmware	Server	1.0.8	All	All	All
Application	Vmware	Server	1.0.9	All	All	All
Application	Vmware	Server	2.0	All	All	All
Application	Vmware	Server	2.0	rc2	All	All
Application	Vmware	Server	2.0.1	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	6.5.0	All	All	All
Application	Vmware	Workstation	6.5.1	All	All	All
Application	Vmware	Workstation	6.5.2	All	All	All

## References

### Reference

SecurityTracker.com Archives - VMware Page Fault Exception Handling Flaw Lets Local Users on a Guest OS Gain Elevated Privileges on the

SecurityFocus

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

VMware Products Guest Privilege Escalation Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

Gentoo Linux Documentation -- VMware Player, Server, Workstation: Multiple vulnerabilities

VMSA-2009-0015

SecurityFocus

[Security-announce] VMSA-2009-0015 VMware hosted products and ESX patches resolve two security issues

VMware Products Page Fault Exception Local Privilege Escalation Vulnerability

Repository / Oval Repository

SecurityTracker.com Archives - VMware ESX Page Fault Exception Handling Flaw Lets Local Users on a Guest OS Gain Elevated Privileges on the

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](#).

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

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