



# CVE-2009-4811

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

## Summary

<b>CVE</b>	CVE-2009-4811
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-04-27 15:30:00 UTC
<b>Updated</b>	2013-05-15 03:04:00 UTC
<b>Description</b>	VMware Authentication Daemon 1.0 in vmware-authd.exe in the VMware Authorization Service in VMware Workstation 7.0

## Risk And Classification

**Problem Types:** CWE-134

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Ace	2.5.0	All	All	All
Application	Vmware	Ace	2.5.1	All	All	All
Application	Vmware	Ace	2.5.2	All	All	All
Application	Vmware	Ace	2.5.3	All	All	All
Application	Vmware	Ace	2.5.4	All	All	All
Application	Vmware	Ace	2.6	All	All	All
Application	Vmware	Ace	2.6.1	All	All	All
Application	Vmware	Ace	2.5.0	All	All	All
Application	Vmware	Ace	2.5.1	All	All	All
Application	Vmware	Ace	2.5.2	All	All	All
Application	Vmware	Ace	2.5.3	All	All	All
Application	Vmware	Ace	2.5.4	All	All	All
Application	Vmware	Ace	2.6	All	All	All
Application	Vmware	Ace	2.6.1	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	3.0	All	All	All
Application	Vmware	Player	3.0.1	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	3.0	All	All	All
Application	Vmware	Player	3.0.1	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	7.0	All	All	All
Application	Vmware	Workstation	7.0.1	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	6.5.3	All	All	All
Application	Vmware	Workstation	6.5.4	All	All	All
Application	Vmware	Workstation	7.0	All	All	All
Application	Vmware	Workstation	7.0.1	All	All	All

## References

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

[Security-announce] VMSA-2010-000/ VMware hosted products, vCenter Server and ESX patches resolve multiple security issues	MLIS I
Free Text Host - The Anonymous Text Hosting Service - No Registration Required	MISC
NEOHAPSIS - Peace of Mind Through Integrity and Insight	BUGTR
VMSA-2010-0007.1	MISC
VMware Player and Workstation 'vmware-authd' Remote Denial of Service Vulnerability	BID
pocoftheday	MISC
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FULLDI
CVE Program record	CVE.OP
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](#)