



CVE-2009-3733

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

Summary

CVE	CVE-2009-3733
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-11-02 15:30:00 UTC
Updated	2018-10-10 19:47:00 UTC
Description	Directory traversal vulnerability in VMware Server 1.x before 1.0.10 build 203137 and 2.x before 2.0.2 build 203138 on Linu

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux	All	All	All	All
Operating System	Linux	Linux	All	All	All	All
Application	Vmware	Esx	3.0.3	All	All	All
Application	Vmware	Esx	3.5	All	All	All
Application	Vmware	Esx	3.0.3	All	All	All
Application	Vmware	Esx	3.5	All	All	All
Application	Vmware	Esxi	3.5	All	All	All
Application	Vmware	Esxi	3.5	All	All	All
Application	Vmware	Server	1.0	All	All	All
Application	Vmware	Server	1.0.1	All	All	All
Application	Vmware	Server	1.0.1_build_29996	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	1.0.4_build_56528	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	2.0.0	All	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	1.0.1_build_29996	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	1.0.4_build_56528	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	2.0.0	All	All	All
Application	Vmware	Server	2.0.1	All	All	All

References						
Reference				Source		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN		
Gentoo Linux Documentation -- VMware Player, Server, Workstation: Multiple vulnerabilities				GENTOO		
VMware Products Directory Traversal Vulnerability				BID		
VMSA-2009-0015				CONFIRM		
SecurityTracker.com Archives - VMware ESX/ESXi Directory Traversal Flaw Lets Remote Users Obtain Arbitrary Files				SECTRAC		
VMware Products Directory Traversal File Disclosure Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA		
SecurityFocus				BUGTRAC		
[Security-announce] VMSA-2009-0015 VMware hosted products and ESX patches resolve two security issues				MLIST		
SecurityTracker.com Archives - VMware Server Directory Traversal Flaw Lets Remote Users Obtain Arbitrary Files				SECTRAC		
Repository / Oval Repository				OVAL		
CVE Program record				CVE.ORG		
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](#)