



CVE-2009-1195

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

Summary

CVE	CVE-2009-1195
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-05-28 20:30:00 UTC
Updated	2023-02-13 02:20:00 UTC
Description	The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the Allow

Risk And Classification

Problem Types: CWE-16

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	-	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.0	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.10	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.2	All	windows	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.3	All	windows	All
Application	Apache	Http Server	2.2.4	All	All	All
Application	Apache	Http Server	2.2.6	All	All	All
Application	Apache	Http Server	2.2.7	All	All	All
Application	Apache	Http Server	2.2.8	All	All	All
Application	Apache	Http Server	2.2.9	All	All	All
Application	Apache	Http Server	-	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.0	All	All	All

Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.10	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.2	All	windows	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.3	All	windows	All
Application	Apache	Http Server	2.2.4	All	All	All
Application	Apache	Http Server	2.2.6	All	All	All
Application	Apache	Http Server	2.2.7	All	All	All
Application	Apache	Http Server	2.2.8	All	All	All
Application	Apache	Http Server	2.2.9	All	All	All
Application	Apache	Http Server	All	All	All	All

References						
Reference					Source	
About Security Update 2009-006 / Mac OS X v10.6.2					CONFIRM	
Pony Mail!					MISC	
Repository / Oval Repository					OVAL	
Pony Mail!					MISC	
Pony Mail!					MISC	
Pony Mail!					MLIST	
Pony Mail!					MLIST	
Apache 'Options' and 'AllowOverride' Directives Security Bypass Vulnerability					BID	
Pony Mail!					MISC	
Pony Mail!					MISC	
Debian update for apache2 - Secunia Advisories - Vulnerability Information - Secunia.com					SECUNIA	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					VUPEN	
Repository / Oval Repository					OVAL	
rhn.redhat.com Red Hat Support					REDHAT	
Repository / Oval Repository					OVAL	
Gentoo update for apache - Secunia Advisories - Vulnerability Information - Secunia.com					SECUNIA	
APPLE-SA-2009-11-09-1 Security Update 2009-006 / Mac OS X v10.6.2					APPLE	
Pony Mail!					MISC	
Support					REDHAT	
Debian -- Security Information -- DSA-1816-1 apache2					DEBIAN	
Pony Mail!					MLIST	

Pony Mail!	MLIS I
Ubuntu update for apache2 - Secunia.com	SECUNIA
Pony Mail!	MLIST
Pony Mail!	MISC
Pony Mail!	MLIST
USN-787-1: Apache vulnerabilities Ubuntu	UBUNTU
Pony Mail!	MISC
Pony Mail!	MLIST
Pony Mail!	MISC
Pony Mail!	MISC
[Apache-SVN] Revision 772997	CONFIRM
SUSE update for apache2 and libapr1 - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
SecurityFocus	BUGTRAQ
Bug 489436 – CVE-2009-1195 httpd: AllowOverride Options=IncludesNoExec allows Options Includes	CONFIRM
Advisories:rPSA-2009-0142 - rPath Wiki	CONFIRM
54733	OSVDB
'[security bulletin] HPSBUX02612 SSRT100345 rev.1 - HP-UX Apache-based Web Server, Local Information' - MARC	HP
SecurityTracker.com Archives - Apache IncludesNoExec Options Restrictions Can Be Bypass By Local Users	SECTRAK
Red Hat update for httpd - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Support / Security / Advisories / / MDVSA-2009:124 Mandriva	MANDRIVA
Pony Mail!	MLIST
Pony Mail!	MLIST
SecurityFocus	BUGTRAQ
Apache HTTP Server AllowOverride Options Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
[security-announce] SUSE Security Announcement: Apache and libapr (SUSE-	SUSE
Gentoo Linux Documentation -- Apache: Multiple vulnerabilities	GENTOO
Pony Mail!	MLIST
'Includes vs IncludesNoExec security issue - help needed' - MARC	MLIST
Pony Mail!	MISC
Pony Mail!	MISC
Pony Mail!	MLIST
[SECURITY] Fedora 11 Update: httpd-2.2.13-1.fc11	FEDORA
Pony Mail!	MLIST
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Pony Mail!	MLIST

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](#)