



CVE-2007-1349

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

Summary

CVE	CVE-2007-1349
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-30 00:19:00 UTC
Updated	2022-02-03 16:26:00 UTC
Description	PerlRun.pm in Apache mod_perl before 1.30, and RegistryCooker.pm in mod_perl 2.x, does not properly escape PATH_IN

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Mod Perl	All	All	All	All
Application	Apache	Mod Perl	All	All	All	All
Application	Apache	Mod Perl	All	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	4.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	4.5	All	All	All

Operating System	Redhat	Enterprise Linux Server	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Application	Redhat	Network Satellite	5.1	All	All	All
Application	Redhat	Network Satellite	5.1	All	All	All
Application	Redhat	Satellite	5.1	All	All	All

References						
Reference				Source	Link	
SUSE Update for Multiple Packages - Advisories - Secunia				SECUNIA	secunia	
1021508				SUNALERT	sunsolv	
Security Announcement				SUSE	www.no	
Red Hat Network Proxy Server update for mod_perl - Advisories - Secunia				SECUNIA	secunia	
rhn.redhat.com Red Hat Support				REDHAT	www.re	
svn.apache.org/repos/asf/perl/modperl/branches/1.x/Changes				CONFIRM	svn.apa	
IBM X-Force Exchange				XF	exchan	
Sun Solaris mod_perl Denial of Service Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA	secunia	
Red Hat update for mod_perl - Advisories - Secunia				SECUNIA	secunia	
20070602-01-P				SGI	patches	
Mod_Pperl Path_Info Remote Denial Of Service Vulnerability				BID	www.se	
Support				REDHAT	www.re	
Ubuntu update for mod_perl - Secunia Advisories - Vulnerability Intelligence - Secunia.com				SECUNIA	secunia	
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia				SECUNIA	secunia	
rhn.redhat.com Red Hat Support				REDHAT	www.re	
Mandriva update for apache-mod_perl - Advisories - Secunia				SECUNIA	secunia	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vl	
USN-1024-1 - Ubuntu Security Notice				UBUNTU	www.ub	

USN-488-1: mod_perl vulnerability Ubuntu	UBUNTU	www.ubuntu.com
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com
rhnl.redhat.com Red Hat Support	REDHAT	rhnl.redhat.com
Repository / Oval Repository	OVAL	oval.cisecurity.com
mod_perl "path_info" Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Red Hat update for mod_perl - Advisories - Secunia	SECUNIA	secunia.com
2007-0023	TRUSTIX	www.trustix.com
Avaya Products mod_perl "path_info" Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Advisories Mandriva	MANDRIVA	www.mandriva.com
Red Hat update for Red Hat Network Satellite Server - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
access.redhat.com	REDHAT	rhnl.redhat.com
Repository / Oval Repository	OVAL	oval.cisecurity.com
rhnl.redhat.com Red Hat Support	REDHAT	www.redhat.com
Sun Solaris mod_perl Denial of Service Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
ASA-2007-293 (RHSA-2007-0486, RHSA-2007-0395)	CONFIRM	support.suse.com
Security Announcement	SUSE	www.novell.com
248386	SUNALERT	sunsolve.oracle.com
Gentoo update for mod_perl - Advisories - Secunia	SECUNIA	secunia.com
Gentoo Linux Documentation -- Apache mod_perl: Denial of Service	GENTOO	security.gentoo.org
Trustix Update for Multiple Packages - Advisories - Secunia	SECUNIA	secunia.com
SecurityTracker.com Archives - mod_perl Input Validation Flaw in PerlRun Module Lets Remote Users Deny Service	SECTRACK	www.securitytracker.com
MP1 Security issue (was Re: [mp1] PerlRun fails if path_info contains special symbols) ModPerl ModPerl	MISC	www.gnss.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)

