



CVE-2011-2767

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

Summary

CVE	CVE-2011-2767
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-26 16:29:00 UTC
Updated	2023-11-07 02:07:00 UTC
Description	mod_perl 2.0 through 2.0.10 allows attackers to execute arbitrary Perl code by placing it in a user-owned .htaccess file, bec

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Mod Perl	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.7	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.3	All	All	All

Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.7	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.3	All	All	All
Operating System	Redhat	Enterprise Linux	7.4	All	All	All
Operating System	Redhat	Enterprise Linux	7.5	All	All	All
Operating System	Redhat	Enterprise Linux	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference	Source
Red Hat Customer Portal	REDHAT
Pony Mail!	
Red Hat Customer Portal	REDHAT
USN-3825-2: mod_perl vulnerability Ubuntu security notices	UBUNTU
Apache 'mod_perl' CVE-2011-2767 Arbitrary Code Execution Vulnerability	BID
[security-announce] openSUSE-SU-2019:2558-1: moderate: Security update f	SUSE
mail-archives.apache.org/mod_mbox/perl-modperl/201110.mbox/raw/%3C20111004084343.GA212...	MISC
USN-3825-1: mod_perl vulnerability Ubuntu security notices	UBUNTU
Pony Mail!	MLIST
#644169 - libapache2-mod-perl2: PerlOptions -Sections not permitted in server config, but should be - Debian Bug report logs	MISC
Red Hat Customer Portal	REDHAT
[security-announce] openSUSE-SU-2019:2549-1: moderate: Security update f	SUSE
[SECURITY] [DLA 1507-1] libapache2-mod-perl2 security update	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](#)