CVE-2009-0796

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-0796
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-07 23:30:00 UTC
Updated	2023-02-13 02:19:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 fo

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Apache	Http Server	All	All	All	All
Application	Apache	Mod Perl	1	All	All	All
Application	Apache	Mod Perl	2	All	All	All
Application	Apache	Mod Perl	1	All	All	All
Application	Apache	Mod Perl	2	All	All	All

References

Reference
1021508
CVE-2009-0796 - Red Hat Customer Portal
APPLE-SA-2010-11-10-1 Mac OS X v10.6.5 and Security Update 2010-007
Support / Security / Advisories / / MDVSA-2009:091 | Mandriva
SecurityFocus
svn commit: r761081 - in /perl/modperl/branches/1.x: Changes lib/Apache/Status.pm | ModPerl | ModPerl-cvs
Repository / Oval Repository
1021709

494402 – (CVE-2009-0796) CVE-2009-0796 httpd mod_perl Apache::Status XSS flaw
Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vulnerability
[Apache-SVN] Diff of /perl/modperl/branches/1.x/lib/Apache/Status.pm
AWS, Azure, Managed Cloud & Security in Canada | Carbon60
mod_perl Input Validation Flaw in Apache::Status and Apache2::Status Permits Cross-Site Scripting Attacks - SecurityTracker
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CVE-2009-0796
[Apache-SVN] Revision 761081
Apache mod_perl "Apache::Status" / "Apache2::Status" Cross-Site Scripting - Secunia Advisories - Vulnerability Information - Secunia.com
About the security content of Mac OS X v10.6.5 and Security Update 2010-007
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-06-11	Tomas Hoger	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com

There are currently no legacy QID mappings associated with this CVE.