



CVE-2012-3499

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

Summary

CVE	CVE-2012-3499
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-26 16:55:00 UTC
Updated	2023-11-07 02:11:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4

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	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	2.2.11	All	All	All
Application	Apache	Http Server	2.2.12	All	All	All
Application	Apache	Http Server	2.2.13	All	All	All
Application	Apache	Http Server	2.2.14	All	All	All
Application	Apache	Http Server	2.2.15	All	All	All
Application	Apache	Http Server	2.2.16	All	All	All
Application	Apache	Http Server	2.2.17	All	All	All
Application	Apache	Http Server	2.2.18	All	All	All
Application	Apache	Http Server	2.2.19	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.22	All	All	All

Application	Apache	Http Server	2.2.23	All	All	All
Application	Apache	Http Server	2.2.3	All	All	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	2.2.8	All	All	All
Application	Apache	Http Server	2.2.9	All	All	All
Application	Apache	Http Server	2.4.0	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.3	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	2.2.11	All	All	All
Application	Apache	Http Server	2.2.12	All	All	All
Application	Apache	Http Server	2.2.13	All	All	All
Application	Apache	Http Server	2.2.14	All	All	All
Application	Apache	Http Server	2.2.15	All	All	All
Application	Apache	Http Server	2.2.16	All	All	All
Application	Apache	Http Server	2.2.17	All	All	All
Application	Apache	Http Server	2.2.18	All	All	All
Application	Apache	Http Server	2.2.19	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.22	All	All	All
Application	Apache	Http Server	2.2.23	All	All	All
Application	Apache	Http Server	2.2.3	All	All	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	2.2.8	All	All	All
Application	Apache	Http Server	2.2.9	All	All	All
Application	Apache	Http Server	2.4.0	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All

Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
References						
Reference				Source	Link	
Pony Mail!				MLIST	lists.ap	
'[security bulletin] HPSBUX02866 SSRT101139 rev.1 - HP-UX Running Apache, Remote Denial of Service (D' - MARC				HP	marc.ir	
Pony Mail!					lists.ap	
Pony Mail!				MLIST	lists.ap	
Pony Mail!				MLIST	lists.ap	
Red Hat Customer Portal				REDHAT	rhn.red	
Pony Mail!				MLIST	lists.ap	
Pony Mail!					lists.ap	
[Apache-SVN] Diff of /httpd/httpd/trunk/modules/mappers/mod_imagemap.c				CONFIRM	svn.ap	
Pony Mail!					lists.ap	
Pony Mail!					lists.ap	
About Secunia Research Flexera				SECUNIA	secunia	
Pony Mail!				MLIST	lists.ap	
Pony Mail!					lists.ap	
APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004				APPLE	lists.ap	
Pony Mail!					lists.ap	
Pony Mail!					lists.ap	
Oracle Critical Patch Update - January 2014				CONFIRM	www.o	
Pony Mail!					lists.ap	
Pony Mail!				MLIST	lists.ap	
Pony Mail!				MLIST	lists.ap	
Pony Mail!				MLIST	lists.ap	
Pony Mail!				MLIST	lists.ap	
[Apache-SVN] Diff of /httpd/httpd/trunk/modules/generators/mod_info.c				CONFIRM	svn.ap	
Pony Mail!					lists.ap	
Pony Mail!				MLIST	lists.ap	
Pony Mail!				MLIST	lists.ap	
Pony Mail!					lists.ap	
Apache HTTP Server Multiple Cross Site Scripting Vulnerabilities				BID	www.s	
Pony Mail!				MLIST	lists.ap	
About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004				CONFIRM	support	

Red Hat Customer Portal	REDHAT	rhn.red
Repository / Oval Repository	OVAL	oval.cis
[Apache-SVN] Diff of /httpd/httpd/trunk/modules/proxy/mod_proxy_ftp.c	CONFIRM	svn.ap
Pony Mail!		lists.ap
[Apache-SVN] Diff of /httpd/httpd/trunk/modules/ldap/util_ldap_cache_mgr.c	CONFIRM	svn.ap
This page provides Security Information. - Fujitsu Global	CONFIRM	www.fu
httpd 2.2 vulnerabilities - The Apache HTTP Server Project	CONFIRM	httpd.a
Pony Mail!		lists.ap
Pony Mail!	MLIST	lists.ap
RETIREd: Oracle January 2014 Critical Patch Update Multiple Vulnerabilities	BID	www.s
Pony Mail!		lists.ap
Pony Mail!	MLIST	lists.ap
Pony Mail!		lists.ap
Red Hat Customer Portal	REDHAT	rhn.red
Pony Mail!		lists.ap
Red Hat Customer Portal	REDHAT	rhn.red
Debian -- Security Information -- DSA-2637-1 apache2	DEBIAN	www.d
Pony Mail!	MLIST	lists.ap
[Apache-SVN] Diff of /httpd/httpd/trunk/modules/generators/mod_status.c	CONFIRM	svn.ap
Pony Mail!	MLIST	lists.ap
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	httpd.a
Pony Mail!		lists.ap
Pony Mail!		lists.ap
[SECURITY] Fedora 18 Update: httpd-2.4.4-2.fc18	FEDORA	lists.fec
Pony Mail!	MLIST	lists.ap
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis



No vendor comments have been submitted for this CVE.

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

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