CVE-2007-4465

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

Summary

CVE	CVE-2007-4465
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-09-14 00:17:00 UTC
Updated	2024-01-19 15:13:00 UTC
Description	Cross-site scripting (XSS) vulnerability in mod_autoindex.c in the Apache HTTP Server before 2.2.6, when the charset on a

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
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	All	All
Application	Apache	Http Server	2.0.34	beta	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All

Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	All	All	All
Application	Apache	Http Server	2.0.56	All	All	All
Application	Apache	Http Server	2.0.57	All	All	All
Application	Apache	Http Server	2.0.58	All	All	All
Application	Apache	Http Server	2.0.59	All	All	All
Application	Apache	Http Server	2.0.60	All	All	All
Application	Apache	Http Server	2.0.61	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.1	All	All	All
Application	Apache	Http Server	2.1.1	All	All	All
Application	Apache	Http Server	2.1.2	All	All	All
Application	Apache	Http Server	2.1.3	All	All	All
Application	Apache	Http Server	2.1.4	All	All	All
Application	Apache	Http Server	2.1.5	All	All	All
Application	Apache	Http Server	2.1.6	All	All	All
Application	Apache	Http Server	2.1.7	All	All	All
Application	Apache	Http Server	2.1.8	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.2	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	-	All	All	All
Application	Apache	Http Server	2.0	All	All	All

Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	All	All
Application	Apache	Http Server	2.0.34	beta	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	All	All	All
Application	Apache	Http Server	2.0.56	All	All	All
Application	Apache	Http Server	2.0.57	All	All	All
Application	Apache	Http Server	2.0.58	All	All	All
Application	Apache	Http Server	2.0.59	All	All	All
Application	Apache	Http Server	2.0.60	All	All	All
Application	Apache	Http Server	2.0.61	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.1	All	All	All
Application	Apache	Http Server	2.1.1	All	All	All

Application	Apache	Http Server	2.1.2	All	All	All
Application	Apache	Http Server	2.1.3	All	All	All
Application	Apache	Http Server	2.1.4	All	All	All
Application	Apache	Http Server	2.1.5	All	All	All
Application	Apache	Http Server	2.1.6	All	All	All
Application	Apache	Http Server	2.1.7	All	All	All
Application	Apache	Http Server	2.1.8	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.4	All	All	All

References

Reference
rhn.redhat.com | Red Hat Support
Advisories | Mandriva
'[security bulletin] HPSBUX02465 SSRT090192 rev.1 - HP-UX Running Apache-based Web Server, Remote Den' - MARC
Red Hat update for apache - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Apache Mod_AutoIndex.C Undefined Charset Cross-Site Scripting Vulnerability
This page provides Security Information. : Fujitsu Global
Fedora update for httpd - Advisories - Secunia
Red Hat update for httpd - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Fedora update for httpd - Advisories - Secunia
rhn.redhat.com | Red Hat Support
IBM X-Force Exchange
Security Announcement
rhn.redhat.com | Red Hat Support
HPSBUX02365 SSRT080118 rev.1 - HP-UX Running Apache, Remote Cross Site Scripting (XSS) or Denial of Service (DoS) - c01539432 - H
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
rhn.redhat.com | Red Hat Support
SecurityReason - Apache2 Undefined Charset UTF-7 XSS Vulnerability
[SECURITY] Fedora Core 6 Update: httpd-2.2.6-1.fc6
rhn.redhat.com | Red Hat Support
Repository / Oval Repository
USN-575-1: Apache vulnerabilities | Ubuntu

Apache Input Validation Hole in Mod_AutoIndex When the Character Set is Undefined May Permit Cross-Site Scripting Attacks - SecurityTrac
Repository / Oval Repository
404 Not Found
US-CERT Technical Cyber Security Alert TA08-150A -- Apple Updates for Multiple Vulnerabilities
Avaya Products httpd Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Gentoo Bug 186219 - www-servers/apache Multiple issues (CVE-2006-{5752}, CVE-2007-{1862,1863,3304,3847,4465})
rhn.redhat.com | Red Hat Support
ASA-2008-032 (RHSA-2008-0006)
HP-UX update for Apache - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
HP-UX Apache Web Server Suite Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
SSRT090085
SUSE update for apache2 - Advisories - Secunia
About Secunia Research | Flexera
Gentoo Linux Documentation -- Apache: Multiple vulnerabilities
APPLE-SA-2008-05-28 Security Update 2008-003 and Mac OS X v10.5.3
SecurityReason - Apache2 Undefined Charset UTF-7 XSS Vulnerability
Ubuntu update for apache2 - Secunia Advisories - Vulnerability Information - Secunia.com
SecurityFocus
Gentoo update for apache - Advisories - Secunia
[SECURITY] Fedora 7 Update: httpd-2.2.6-1.fc7
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-09-18	Mark J Cox	This is actually a flaw in browsers that do not derive the response character set as required by R
Apache	2007-09-14	Mark J Cox	The Apache security team believe that this issue is due to web browsers that are violating RFC2

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**