CVE-2007-6203

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

Summary

CVE	CVE-2007-6203
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-03 22:46:00 UTC
Updated	2018-10-15 21:50:00 UTC
Description	Apache HTTP Server 2.0.x and 2.2.x does not sanitize the HTTP Method specifier header from an HTTP request when it is

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	2.0.46	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	2.0.57	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	2.1.1	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	2.2.0	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	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	2.0.57	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	2.1.1	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	2.2.0	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	Source
Repository / Oval Repository	OVAL
SUSE update for apache and apache2 - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
'[security bulletin] HPSBUX02465 SSRT090192 rev.1 - HP-UX Running Apache-based Web Server, Remote Den' - MARC	HP
About Security Update 2008-002	CONFIRM
This page provides Security Information. : Fujitsu Global	CONFIRM
IBM PK65782; 2.0.47.1: IBM HTTP Server V2.0.47 Cumulative Interim Fix - United States	AIXAPAR
IBM HTTP Server Two Cross-Site Scripting Vulnerabilities - Advisories - Secunia	SECUNIA
Apache: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO
ProCheckUp - Security Vulnerabilities 2007	MISC
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SecurityReason - XSS on Apache HTTP Server 413 error pages via malformed HTTP method	SREASON
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Gentoo update for apache - Advisories - Secunia	SECUNIA
'[security bulletin] HPSBUX02612 SSRT100345 rev.1 - HP-UX Apache-based Web Server, Local Information' - MARC	HP
IBM HTTP Server Multiple Cross-Site Scripting Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Apache HTTP Server 413 Error HTTP Request Method Cross-Site Scripting Weakness	BID
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Apache HTTP Method Request Entity Too Large Cross-Site Scripting - Advisories - Secunia	SECUNIA
Security Alerts - Secunia	SECUNIA
USN-731-1: Apache vulnerabilities | Ubuntu	UBUNTU
IBM PK57952: INPUT METHOD NOT ESCAPED IN DEFAULT 413 ERROR RESPONSE - United States	AIXAPAR
[security-announce] SUSE Security Announcement: Apache,Apache2 security	SUSE
About Secunia Research | Flexera	SECUNIA
IBM HMC Apache Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
APPLE-SA-2008-03-18 Security Update 2008-002	APPLE
Apache Input Validation Hole in Default HTTP 413 Error Page Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK
SecurityFocus	BUGTRAQ
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-06-09	Mark J Cox	The Apache Software Foundation security team does not consider this issue to be a security vul
Red Hat	2007-12-06	Mark J Cox	Red Hat does not consider this issue to be a vulnerability. In order to exploit this for cross-site sc

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**