



CVE-2002-0392

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

Summary

CVE	CVE-2002-0392
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-07-03 04:00:00 UTC
Updated	2023-11-07 01:55:00 UTC
Description	Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possib

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	1.0	All	All	All
Application	Apache	Http Server	1.0.2	All	All	All
Application	Apache	Http Server	1.0.3	All	All	All
Application	Apache	Http Server	1.0.5	All	All	All
Application	Apache	Http Server	1.1	All	All	All
Application	Apache	Http Server	1.1.1	All	All	All
Application	Apache	Http Server	1.2	All	All	All
Application	Apache	Http Server	1.2.5	All	All	All
Application	Apache	Http Server	1.3	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All
Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.11	All	win32	All
Application	Apache	Http Server	1.3.12	All	All	All
Application	Apache	Http Server	1.3.12	All	win32	All
Application	Apache	Http Server	1.3.13	All	win32	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.14	All	mac_os	All

Application	Apache	Http Server	1.3.14	All	win32	All
Application	Apache	Http Server	1.3.15	All	win32	All
Application	Apache	Http Server	1.3.16	All	win32	All
Application	Apache	Http Server	1.3.17	All	All	All
Application	Apache	Http Server	1.3.17	All	win32	All
Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.18	All	win32	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.19	All	win32	All
Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.20	All	win32	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.22	All	win32	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.23	All	win32	All
Application	Apache	Http Server	1.3.24	All	All	All
Application	Apache	Http Server	1.3.24	All	win32	All
Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.9	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	2.0.32	All	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	1.0	All	All	All
Application	Apache	Http Server	1.0.2	All	All	All
Application	Apache	Http Server	1.0.3	All	All	All
Application	Apache	Http Server	1.0.5	All	All	All
Application	Apache	Http Server	1.1	All	All	All
Application	Apache	Http Server	1.1.1	All	All	All
Application	Apache	Http Server	1.2	All	All	All
Application	Apache	Http Server	1.2.5	All	All	All
Application	Apache	Http Server	1.3	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All

Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.11	All	win32	All
Application	Apache	Http Server	1.3.12	All	All	All
Application	Apache	Http Server	1.3.12	All	win32	All
Application	Apache	Http Server	1.3.13	All	win32	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.14	All	mac_os	All
Application	Apache	Http Server	1.3.14	All	win32	All
Application	Apache	Http Server	1.3.15	All	win32	All
Application	Apache	Http Server	1.3.16	All	win32	All
Application	Apache	Http Server	1.3.17	All	All	All
Application	Apache	Http Server	1.3.17	All	win32	All
Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.18	All	win32	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.19	All	win32	All
Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.20	All	win32	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.22	All	win32	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.23	All	win32	All
Application	Apache	Http Server	1.3.24	All	All	All
Application	Apache	Http Server	1.3.24	All	win32	All
Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.9	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	2.0.32	All	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	All	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Debian	Debian Linux	2.2	All	All	All

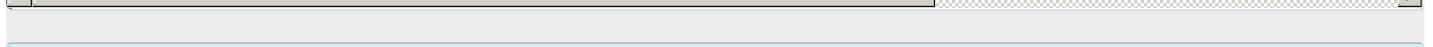
References	
Reference	Source
SSRT050968	HP
Pony Mail!	MLIST
Security Announcement	SUSE
838	OSVDB
Pony Mail!	
httpd.apache.org/info/security_bulletin_20020617.txt	CONFIRM
Pony Mail!	
redhat.com Red Hat Support	REDHAT
frontal2.mandriva.com	MANDRAKE
Pony Mail!	MLIST
redhat.com Red Hat Support	REDHAT
Pony Mail!	
Pony Mail!	
SecurityFocus HOME Mailing List: BugTraq	BUGTRAQ
Pony Mail!	
CSSA-2002-029.0	CALDERA
CERT Advisory CA-2002-17 Apache Web Server Chunk Handling Vulnerability	CERT
Pony Mail!	
Pony Mail!	MLIST
redhat.com Red Hat Support	REDHAT
CSSA-2002-SCO.31	CALDERA
20020605-01-A	SGI
redhat.com Red Hat Support	REDHAT
Neohapsis Archives - Bugtraq - [OpenPKG-SA-2002.004] OpenPKG Security Advisory (apache) - From openpkgopenpkg.org	BUGTRAQ
Pony Mail!	MLIST
Pony Mail!	
SecurityFocus HOME Advisories: Security vulnerability in Apache	HP
HP OpenView Operations Apache Chunked Encoding Vulnerability - Advisories - Secunia	SECUNIA
Apache Chunked-Encoding Memory Corruption Vulnerability	BID
Debian -- Security Information -- DSA-132-1 apache-ssl	DEBIAN
SecurityFocus HOME Advisories: Sec. Vulnerability in Apache Server Chunk Encodi	HP
Pony Mail!	MLIST
Pony Mail!	

Debian -- Security Information -- DSA-131-1 apache	DEBIAN
ISS X-Force Database: apache-chunked-encoding-bo (9249): Apache HTTP Server chunked encoding heap buffer overflow	XF
Félicitations ! Votre domaine a bien été créé chez OVH !	FRSIRT
Pony Mail!	
20020605-01-I	SGI
Pony Mail!	
HP OpenView Operations Denial of Service and Unauthorized Access Vulnerability	BID
redhat.com Red Hat Support	REDHAT
CSSA-2002-SCO.32	CALDERA
Debian -- Security Information -- DSA-133-1 apache-perl	DEBIAN
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	
LinuxSecurity.com: EnGarde: 'apache' chunk handling overflow vulnerability	ENGARDE
redhat.com Red Hat Support	REDHAT
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	MLIST
Neohapsis Archives - Bugtraq - [slackware-security] new apache/mod_ssl packages available - From dasecurityfocus.com	BUGTRAQ
CLSA-2002:498	CONNECTIVA
Pony Mail!	MLIST
Pony Mail!	
CERT/CC Vulnerability Note VU#944335	CERT-VN
Pony Mail!	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.0.37 and 1.3.26: http://httpd.apache.org/security/vulnerabilities_



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

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