

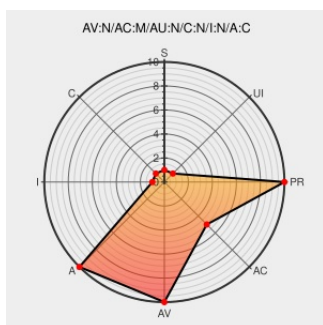


CVE-2009-1891

Published on: 07/10/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:20:00 AM UTC

CVE-2009-1891

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

CVE-2009-1891 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.1 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

About Security Update 2009-006 / Mac OS X v10.6.2

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[CONFIRM support.apple.com/kb/HT3937](#)

Pony Mail!

[lists.apache.org](#)

[text/html](#)

MLIST [httpd-cvs] 20190815 svn commit: r1048742 [3/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html

Pony Mail!

[lists.apache.org](#)

[text/html](#)

MLIST [httpd-cvs] 20210330 svn commit: r1073139 [5/13] - in /websites/staging/httpd/trunk/content: ./ security/json/

IBM PK99480: SHIP APAR FIXES FOR H28W700 FIX PACK 7.0.0.7. - United States

[www-01.ibm.com](#)

[text/html](#)

[AIXAPAR PK99480](#)

Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073140 [3/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20200401 svn commit: r1058587 [3/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
rhn.redhat.com Red Hat Support	Patch web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2009:1148
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073149 [6/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
Red Hat update for httpd - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 35793
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210603 svn commit: r1075360 [1/3] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20200401 svn commit: r1058586 [3/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
'Re: mod_deflate DoS' - MARC	marc.info text/html	 MLIST [apache-httpd-dev] 20090703 Re: mod_deflate DoS
Advisories:rPSA-2009-0142 - rPath Wiki	web.archive.org text/html Inactive Link Not Archived	 CONFIRM wiki.rpath.com/wiki/Advisories:rPSA-2009-0142
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20200401 svn commit: r1058586 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Advisories Mandriva	Patch www.mandriva.com text/html	 MANDRIVA MDVSA-2009:149
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20190815 svn commit: r1048742 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2009:1156
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20200401 svn commit: r1058587 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html

Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r10/3140 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Gentoo update for apache - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 35721
APPLE-SA-2009-11-09-1 Security Update 2009-006 / Mac OS X v10.6.2	lists.apple.com text/html	 APPLE APPLE-SA-2009-11-09-1
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073146 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities-httpd.xml security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210606 svn commit: r1075470 [3/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20190815 svn commit: r1048743 [3/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:12361
About Secunia Research Flexera	Vendor Advisory web.archive.org text/html	 SECUNIA 35781
IBM WebSphere Application Server for z/OS Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 37221
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1888194 [5/13] - /httpd/site/trunk/content/security/json/
#534712 - apache2.2-common: DOS possible with mod_deflate - Debian Bug report logs	Exploit bugs.debian.org text/html	 MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=534712
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2009-1841
SUSE update for apache2 and libapr1 - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 37152
'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC	marc.info text/html	 HP SSRT090208
SecurityFocus	www.securityfocus.com	 BUGTRAQ 20091113 rPSA-2009-0142-2 httpd mod_ssl

	text/html	
	Exploit marc.info text/x-diff	 MLIST [apache-httpd-dev] 20090628 mod_deflate DoS
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20190815 svn commit: r1048743 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Advisories:rPSA-2009-0142 - rPath Wiki	web.archive.org text/html Inactive Link Not Archived	 CONFIRM wiki.rpath.com/Advisories:rPSA-2009-0142
IBM PK91361: CVE-2009-1891: MOD_DEFLATE - United States	www-01.ibm.com text/html	 AIXAPAR PK91361
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:8632
'[security bulletin] HPSBUX02612 SSRT100345 rev.1 - HP-UX Apache-based Web Server, Local Information' - MARC	marc.info text/html	 HP HPSBUX02612
SecurityTracker.com Archives - Apache mod_deflate Connection State Bug Lets Remote Users Deny Service	www.securitytracker.com text/html	 SECTrack 1022529
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210603 svn commit: r1075360 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:9248
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210606 svn commit: r1075467 [1/2] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
[security-announce] SUSE Security Announcement: Apache and libapr (SUSE-	lists.opensuse.org text/html	 SUSE SUSE-SA:2009:050
Gentoo Linux Documentation -- Apache: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-200907-04
Bug 509125 – CVE-2009-1891 httpd: possible temporary DoS (CPU consumption) in mod_deflate	Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=509125
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073149 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
[SECURITY] Fedora 11 Update: httpd-2.2.13-1.fc11	www.redhat.com text/html	 FEDORA FEDORA-2009-8812
Debian update for apache2 - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 35865
USN-802-1: Apache vulnerabilities	www.ubuntu.com	 UBUNTU USN-802-1

Ubuntu	text/html	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-3184
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 55782
Debian -- Security Information -- DSA-1834-1 apache2	www.debian.org Depreciated Link text/html	DEBIAN DSA-1834
Pony Mail!	lists.apache.org text/html	MLIST [httpd-cvs] 20210606 svn commit: r1075470 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	0.8.11	All	All	All
Application	Apache	Http Server	0.8.14	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	1.2.4	All	All	All
Application	Apache	Http Server	1.2.9	All	All	All
Application	Apache	Http Server	1.3.13	All	All	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.20	All	All	All

Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.29	All	All	All
Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.33	All	All	All
Application	Apache	Http Server	1.3.38	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.7	All	All	All
Application	Apache	Http Server	1.3.9	All	All	All
Application	Apache	Http Server	1.99	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.34	beta	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	2.0.45	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	2.1.9	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	2.2.2	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	2.2.6	All	All	All
Application	Apache	Http Server	2.2.7	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	-	All	All	All
Application	Apache	Http Server	0.8.11	All	All	All
Application	Apache	Http Server	0.8.14	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	1.2.4	All	All	All
Application	Apache	Http Server	1.2.9	All	All	All
Application	Apache	Http Server	1.3.13	All	All	All
Application	Apache	Http Server	1.3.14	All	All	All

Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.29	All	All	All
Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.33	All	All	All
Application	Apache	Http Server	1.3.38	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.7	All	All	All
Application	Apache	Http Server	1.3.9	All	All	All
Application	Apache	Http Server	1.99	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.34	beta	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	2.0.45	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	2.0.58	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	2.1.9	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	2.2.2	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	2.2.6	All	All	All
Application	Apache	Http Server	2.2.7	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	All	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All

ማግኘት

Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Fedoraproject	Fedora	11	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.3	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All

```
cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:-:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:0.8.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:0.8.14:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.0.3:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.1:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.2.*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.2.4:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.2.9:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.14:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.18:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.19:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.20:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.22:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.23:*:*:*:*:*:*
```

cpe:2.3:a:apache:http_server:1.3.27:*****:
cpe:2.3:a:apache:http_server:1.3.29:*****:
cpe:2.3:a:apache:http_server:1.3.3:*****:
cpe:2.3:a:apache:http_server:1.3.31:*****:
cpe:2.3:a:apache:http_server:1.3.33:*****:
cpe:2.3:a:apache:http_server:1.3.38:*****:
cpe:2.3:a:apache:http_server:1.3.6:*****:
cpe:2.3:a:apache:http_server:1.3.7:*****:
cpe:2.3:a:apache:http_server:1.3.9:*****:
cpe:2.3:a:apache:http_server:1.99:*****:
cpe:2.3:a:apache:http_server:2.0.28:*****:
cpe:2.3:a:apache:http_server:2.0.34:beta:*****:
cpe:2.3:a:apache:http_server:2.0.38:*****:
cpe:2.3:a:apache:http_server:2.0.39:*****:
cpe:2.3:a:apache:http_server:2.0.40:*****:
cpe:2.3:a:apache:http_server:2.0.41:*****:
cpe:2.3:a:apache:http_server:2.0.42:*****:
cpe:2.3:a:apache:http_server:2.0.45:*****:
cpe:2.3:a:apache:http_server:2.0.46:*****:
cpe:2.3:a:apache:http_server:2.0.47:*****:
cpe:2.3:a:apache:http_server:2.0.48:*****:
cpe:2.3:a:apache:http_server:2.0.49:*****:
cpe:2.3:a:apache:http_server:2.0.50:*****:
cpe:2.3:a:apache:http_server:2.0.51:*****:
cpe:2.3:a:apache:http_server:2.0.52:*****:
cpe:2.3:a:apache:http_server:2.0.53:*****:
cpe:2.3:a:apache:http_server:2.0.54:*****:
cpe:2.3:a:apache:http_server:2.0.55:*****:
cpe:2.3:a:apache:http_server:2.0.56:*****:

cpe:2.3:a:apache:http_server:2.0.57:*****:
cpe:2.3:a:apache:http_server:2.0.58:*****:
cpe:2.3:a:apache:http_server:2.0.59:*****:
cpe:2.3:a:apache:http_server:2.0.60:*****:
cpe:2.3:a:apache:http_server:2.0.61:*****:
cpe:2.3:a:apache:http_server:2.0.9:*****:
cpe:2.3:a:apache:http_server:2.1:*****:
cpe:2.3:a:apache:http_server:2.1.1:*****:
cpe:2.3:a:apache:http_server:2.1.2:*****:
cpe:2.3:a:apache:http_server:2.1.3:*****:
cpe:2.3:a:apache:http_server:2.1.4:*****:
cpe:2.3:a:apache:http_server:2.1.5:*****:
cpe:2.3:a:apache:http_server:2.1.6:*****:
cpe:2.3:a:apache:http_server:2.1.7:*****:
cpe:2.3:a:apache:http_server:2.1.8:*****:
cpe:2.3:a:apache:http_server:2.1.9:*****:
cpe:2.3:a:apache:http_server:2.2:*****:
cpe:2.3:a:apache:http_server:2.2.0:*****:
cpe:2.3:a:apache:http_server:2.2.1:*****:
cpe:2.3:a:apache:http_server:2.2.10:*****:
cpe:2.3:a:apache:http_server:2.2.2:*****:
cpe:2.3:a:apache:http_server:2.2.3:*****:
cpe:2.3:a:apache:http_server:2.2.4:*****:
cpe:2.3:a:apache:http_server:2.2.6:*****:
cpe:2.3:a:apache:http_server:2.2.7:*****:
cpe:2.3:a:apache:http_server:2.2.8:*****:
cpe:2.3:a:apache:http_server:2.2.9:*****:
cpe:2.3:a:apache:http_server:-:*****:

cpe:2.3:a:apache:http_server:0.8.11:*****:
cpe:2.3:a:apache:http_server:0.8.14:*****:
cpe:2.3:a:apache:http_server:1.0.2:*****:
cpe:2.3:a:apache:http_server:1.0.3:*****:
cpe:2.3:a:apache:http_server:1.0.5:*****:
cpe:2.3:a:apache:http_server:1.1:*****:
cpe:2.3:a:apache:http_server:1.1.1:*****:
cpe:2.3:a:apache:http_server:1.2:*****:
cpe:2.3:a:apache:http_server:1.2.4:*****:
cpe:2.3:a:apache:http_server:1.2.9:*****:
cpe:2.3:a:apache:http_server:1.3.13:*****:
cpe:2.3:a:apache:http_server:1.3.14:*****:
cpe:2.3:a:apache:http_server:1.3.18:*****:
cpe:2.3:a:apache:http_server:1.3.19:*****:
cpe:2.3:a:apache:http_server:1.3.20:*****:
cpe:2.3:a:apache:http_server:1.3.22:*****:
cpe:2.3:a:apache:http_server:1.3.23:*****:
cpe:2.3:a:apache:http_server:1.3.27:*****:
cpe:2.3:a:apache:http_server:1.3.29:*****:
cpe:2.3:a:apache:http_server:1.3.3:*****:
cpe:2.3:a:apache:http_server:1.3.31:*****:
cpe:2.3:a:apache:http_server:1.3.33:*****:
cpe:2.3:a:apache:http_server:1.3.38:*****:
cpe:2.3:a:apache:http_server:1.3.6:*****:
cpe:2.3:a:apache:http_server:1.3.7:*****:
cpe:2.3:a:apache:http_server:1.3.9:*****:
cpe:2.3:a:apache:http_server:1.99:*****:
cpe:2.3:a:apache:http_server:2.0.28:*****:
cpe:2.3:a:apache:http_server:2.0.34:beta:*****:

cpe:2.3:a:apache:http_server:2.0.38:*****:
cpe:2.3:a:apache:http_server:2.0.39:*****:
cpe:2.3:a:apache:http_server:2.0.40:*****:
cpe:2.3:a:apache:http_server:2.0.41:*****:
cpe:2.3:a:apache:http_server:2.0.42:*****:
cpe:2.3:a:apache:http_server:2.0.45:*****:
cpe:2.3:a:apache:http_server:2.0.46:*****:
cpe:2.3:a:apache:http_server:2.0.47:*****:
cpe:2.3:a:apache:http_server:2.0.48:*****:
cpe:2.3:a:apache:http_server:2.0.49:*****:
cpe:2.3:a:apache:http_server:2.0.50:*****:
cpe:2.3:a:apache:http_server:2.0.51:*****:
cpe:2.3:a:apache:http_server:2.0.52:*****:
cpe:2.3:a:apache:http_server:2.0.53:*****:
cpe:2.3:a:apache:http_server:2.0.54:*****:
cpe:2.3:a:apache:http_server:2.0.55:*****:
cpe:2.3:a:apache:http_server:2.0.56:*****:
cpe:2.3:a:apache:http_server:2.0.57:*****:
cpe:2.3:a:apache:http_server:2.0.58:*****:
cpe:2.3:a:apache:http_server:2.0.59:*****:
cpe:2.3:a:apache:http_server:2.0.60:*****:
cpe:2.3:a:apache:http_server:2.0.61:*****:
cpe:2.3:a:apache:http_server:2.0.9:*****:
cpe:2.3:a:apache:http_server:2.1:*****:
cpe:2.3:a:apache:http_server:2.1.1:*****:
cpe:2.3:a:apache:http_server:2.1.2:*****:
cpe:2.3:a:apache:http_server:2.1.3:*****:
cpe:2.3:a:apache:http_server:2.1.4:*****:

cpe:2.3:a:apache:http_server:2.1.5:*****:
cpe:2.3:a:apache:http_server:2.1.6:*****:
cpe:2.3:a:apache:http_server:2.1.7:*****:
cpe:2.3:a:apache:http_server:2.1.8:*****:
cpe:2.3:a:apache:http_server:2.1.9:*****:
cpe:2.3:a:apache:http_server:2.2:*****:
cpe:2.3:a:apache:http_server:2.2.0:*****:
cpe:2.3:a:apache:http_server:2.2.1:*****:
cpe:2.3:a:apache:http_server:2.2.10:*****:
cpe:2.3:a:apache:http_server:2.2.2:*****:
cpe:2.3:a:apache:http_server:2.2.3:*****:
cpe:2.3:a:apache:http_server:2.2.4:*****:
cpe:2.3:a:apache:http_server:2.2.6:*****:
cpe:2.3:a:apache:http_server:2.2.7:*****:
cpe:2.3:a:apache:http_server:2.2.8:*****:
cpe:2.3:a:apache:http_server:2.2.9:*****:
cpe:2.3:a:apache:http_server:*****:
cpe:2.3:o:canonical:ubuntu_linux:6.06:*****:
cpe:2.3:o:canonical:ubuntu_linux:8.04:***:-***:
cpe:2.3:o:canonical:ubuntu_linux:8.10:*****:
cpe:2.3:o:canonical:ubuntu_linux:9.04:*****:
cpe:2.3:o:debian:debian_linux:4.0:*****:
cpe:2.3:o:debian:debian_linux:5.0:*****:
cpe:2.3:o:debian:debian_linux:6.0:*****:
cpe:2.3:o:fedoraproject:fedora:11:*****:
cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*****:
cpe:2.3:o:redhat:enterprise_linux_eus:5.3:*****:
cpe:2.3:o:redhat:enterprise_linux_server:5.0:*****:
cpe:2.3:o:redhat:enterprise_linux_server_aus:5.3:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus:5.0:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)