



CVE-2011-4317

Published on: 11/29/2011 12:00:00 AM UTC

Last Modified on: 06/06/2021 11:15:00 AM UTC

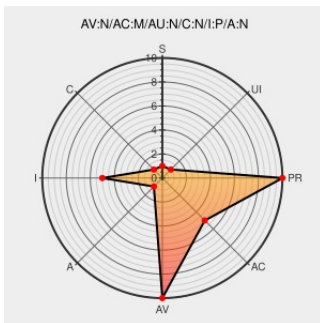
CVE-2011-4317

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send

requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVE-2011-4317 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

**Access
Vector**

NETWORK

**Access
Complexity**

MEDIUM

Authentication

NONE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

PARTIAL

**Availability
Impact**

NONE

CVE References

Description

Tags

Link

HPSBMU02786 SSRT100877 rev.2 - HP System Management Homepage (SMH) Running on Linux, Windows, and VMware ESX, Remote Unauthorized Access, Disclosure of Information, Data Modification, Denial of Service (DoS), Execution of Arbitrary Code - c03360041 - HP Business Support Center

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[HP HPSBMU02786](#)

openSUSE-SU-2013:0248-1: moderate:

[lists.opensuse.org](#)

[SUSE openSUSE-SU-2013:0248](#)

update for apache2	text/html	
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1888194 [8/13] - /httpd/site/trunk/content/security/json/
Gmane Loom	Exploit web.archive.org text/html Inactive Link Not Archived	 CONFIRM thread.gmane.org/gmane.comp.apache.devel/46440
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [8/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
Debian -- Security Information -- DSA-2405-1 apache2	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2405
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
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
Juniper Networks - 2013-08 Security Bulletin: Junos Space: Multiple Vulnerabilities - Knowledge Base	kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA10585
Apache HTTP Server Reverse Proxy/Rewrite URL Validation Issue Qualys Security Labs Qualys Community	Exploit community.qualys.com text/html	 MISC community.qualys.com/blogs/securitylabs/2011/11/23/apache-reverse-proxy-bypass-issue
APPLE-SA-2012-09-19-2 OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004	lists.apple.com text/html	 APPLE APPLE-SA-2012-09-19-2
Bug 756483 – CVE-2011-4317 httpd: uri scheme bypass of the reverse proxy vulnerability CVE-2011-3368 fix	bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=756483
About the security content of OS X Mountain Lion v10.8.2, OS X Lion v10.7.5 and Security Update 2012-004	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT5501
openSUSE-SU-2013:0243-1: moderate: update for apache2	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0243
Apache mod_proxy/mod_rewrite Bug Lets Remote Users Access Internal Servers - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1026353
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073140 [3/4] - 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
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073149 [8/13] - in /websites/staging/httpd/trunk/content: ./ security/security/json/
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] 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
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073146 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohml.py security/vulnerabilities-httpd.xml security/vulnerabilities_22.html security/vulnerabilities_24.html
Support / Security / Advisories // MDVSA-2012:003 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2012:003
Oracle Critical Patch Update - January 2015	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
Security Alerts - Secunia	web.archive.org text/html	 SECUNIA 48551
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210606 svn commit: r1075467 [2/2] - 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
Support / Security / Advisories // MDVSA-2013:150 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2013:150
'[security bulletin] HPSBMU02748 SSRT100772 rev.1 - HP OpenView Network Node Manager (OV NNM) Running' - MARC	marc.info text/html	 HP SSRT100772
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
'[security bulletin] HPSBOV02822 SSRT100966 rev.1 - HP Secure Web Server (SWS) for OpenVMS, Remote De' - MARC	marc.info text/html	 HP SSRT100966
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
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/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0128
Oracle Critical Patch Update - July 2012	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
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

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	1.3	All	All	All
Application	Apache	Http Server	1.3.0	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All
Application	Apache	Http Server	1.3.1.1	All	All	All
Application	Apache	Http Server	1.3.10	All	All	All
Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.12	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	1.3.15	All	All	All
Application	Apache	Http Server	1.3.16	All	All	All
Application	Apache	Http Server	1.3.17	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	1.3.2	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	1.3.24	All	All	All
Application	Apache	Http Server	1.3.25	All	All	All
Application	Apache	Http Server	1.3.26	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.28	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	1.3.30	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All

Application	Apache	Http Server	1.3.32	All	All	All
Application	Apache	Http Server	1.3.33	All	All	All
Application	Apache	Http Server	1.3.34	All	All	All
Application	Apache	Http Server	1.3.35	All	All	All
Application	Apache	Http Server	1.3.36	All	All	All
Application	Apache	Http Server	1.3.37	All	All	All
Application	Apache	Http Server	1.3.38	All	All	All
Application	Apache	Http Server	1.3.39	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.41	All	All	All
Application	Apache	Http Server	1.3.42	All	All	All
Application	Apache	Http Server	1.3.5	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.65	All	All	All
Application	Apache	Http Server	1.3.68	All	All	All
Application	Apache	Http Server	1.3.7	All	All	All
Application	Apache	Http Server	1.3.8	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	2.0.28	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	2.0.47	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	2.0.63	All	All	All
Application	Apache	Http Server	2.0.64	All	All	All
Application	Apache	Http Server	2.0.9	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	2.2.18	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	2.2.3	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	1.3	All	All	All
Application	Apache	Http Server	1.3.0	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All
Application	Apache	Http Server	1.3.1.1	All	All	All
Application	Apache	Http Server	1.3.10	All	All	All
Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.12	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	1.3.15	All	All	All
Application	Apache	Http Server	1.3.16	All	All	All
Application	Apache	Http Server	1.3.17	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	1.3.2	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	1.3.24	All	All	All
Application	Apache	Http Server	1.3.25	All	All	All
Application	Apache	Http Server	1.3.26	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.28	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	1.3.30	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.32	All	All	All
Application	Apache	Http Server	1.3.33	All	All	All
Application	Apache	Http Server	1.3.34	All	All	All
Application	Apache	Http Server	1.3.35	All	All	All
Application	Apache	Http Server	1.3.36	All	All	All
Application	Apache	Http Server	1.3.37	All	All	All

Application	Apache	Http Server	1.3.38	All	All	All
Application	Apache	Http Server	1.3.39	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.41	All	All	All
Application	Apache	Http Server	1.3.42	All	All	All
Application	Apache	Http Server	1.3.5	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.65	All	All	All
Application	Apache	Http Server	1.3.68	All	All	All
Application	Apache	Http Server	1.3.7	All	All	All
Application	Apache	Http Server	1.3.8	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	2.0.28	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	2.0.63	All	All	All
Application	Apache	Http Server	2.0.64	All	All	All
Application	Apache	Http Server	2.0.9	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	2.2.18	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	2.2.3	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
cpe:2.3:a:apache:http_server:1.3:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:1.3.0:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:1.3.1:*:*:*:*:*:						

```
cpe:2.3:a:apache:http_server:1.3.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.12:*:*:*:*:*:*:
```

```
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:1.3.15:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.16:*:*:*:*:*:*
```

```
cpe:2.3:a:apache:http_server:1.3.17:*:*:*:*:*:*:
```

```
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:1.3.2:*:*:*:*:*:*:
```

```
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:1.3.24:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.25:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.26:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.27:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.28:*:*:*:*:*:*:
```

```
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:1.3.30:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.31:::*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.32:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.33:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.34:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.35:*:*:*:*:*:*
```

```
cpe:2.3:a:apache:httn_server:1.3.36:*:*:*:*:*.*
```

cpe:2.3:a:apache:http_server:1.3.37:****:*
cpe:2.3:a:apache:http_server:1.3.37:****:*
cpe:2.3:a:apache:http_server:1.3.38:****:*
cpe:2.3:a:apache:http_server:1.3.39:****:*
cpe:2.3:a:apache:http_server:1.3.4:****:*
cpe:2.3:a:apache:http_server:1.3.41:****:*
cpe:2.3:a:apache:http_server:1.3.42:****:*
cpe:2.3:a:apache:http_server:1.3.5:****:*
cpe:2.3:a:apache:http_server:1.3.6:****:*
cpe:2.3:a:apache:http_server:1.3.65:****:*
cpe:2.3:a:apache:http_server:1.3.68:****:*
cpe:2.3:a:apache:http_server:1.3.7:****:*
cpe:2.3:a:apache:http_server:1.3.8:****:*
cpe:2.3:a:apache:http_server:1.3.9:****:*
cpe:2.3:a:apache:http_server:2.0:****:*
cpe:2.3:a:apache:http_server:2.0.28:****:*
cpe:2.3:a:apache:http_server:2.0.28:beta:****:*
cpe:2.3:a:apache:http_server:2.0.32:****:*
cpe:2.3:a:apache:http_server:2.0.32:beta:****:*
cpe:2.3:a:apache:http_server:2.0.34:beta:****:*
cpe:2.3:a:apache:http_server:2.0.35:****:*
cpe:2.3:a:apache:http_server:2.0.36:****:*
cpe:2.3:a:apache:http_server:2.0.37:****:*
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:2.0.43:****:*

cpe:2.3:a:apache:http_server:2.0.44:*****:
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:2.0.63:*****:
cpe:2.3:a:apache:http_server:2.0.64:*****:
cpe:2.3:a:apache:http_server:2.0.9:*****:
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:2.2.11:*****:
cpe:2.3:a:apache:http_server:2.2.12:*****:
cpe:2.3:a:apache:http_server:2.2.13:*****:
cpe:2.3:a:apache:http_server:2.2.14:*****:
cpe:2.3:a:apache:http_server:2.2.15:*****:

cpe:2.3:a:apache:http_server:2.2.15:*****:
cpe:2.3:a:apache:http_server:2.2.16:*****:
cpe:2.3:a:apache:http_server:2.2.18:*****:
cpe:2.3:a:apache:http_server:2.2.19:*****:
cpe:2.3:a:apache:http_server:2.2.2:*****:
cpe:2.3:a:apache:http_server:2.2.20:*****:
cpe:2.3:a:apache:http_server:2.2.21:*****:
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:2.2.8:*****:
cpe:2.3:a:apache:http_server:2.2.9:*****:
cpe:2.3:a:apache:http_server:1.3:*****:
cpe:2.3:a:apache:http_server:1.3.0:*****:
cpe:2.3:a:apache:http_server:1.3.1:*****:
cpe:2.3:a:apache:http_server:1.3.1.1:*****:
cpe:2.3:a:apache:http_server:1.3.10:*****:
cpe:2.3:a:apache:http_server:1.3.11:*****:
cpe:2.3:a:apache:http_server:1.3.12:*****:
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:1.3.15:*****:
cpe:2.3:a:apache:http_server:1.3.16:*****:
cpe:2.3:a:apache:http_server:1.3.17:*****:
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:1.3.2:*****:
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:1.3.24:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.25:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.26:::*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.27:::*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.28:*:*:*:*:*:
```

```
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:1.3.30:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.31:::*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.32:*:*:*:*:*:*
```

```
cpe:2.3:a:apache:http_server:1.3.33:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.34:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.35:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.36:*:*:*:*:*:*
```

```
cpe:2.3:a:apache:http_server:1.3.37:::*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.38:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:apache:http_server:1.3.39:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.4:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.41:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.42:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.5:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.6:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:apache:http_server:1.3.65:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.68:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.7:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:http_server:1.3.9:*:*:*:*:*:*:
```

cpe:2.3:a:apache:http_server:2.0:*****:
cpe:2.3:a:apache:http_server:2.0.28:*****:
cpe:2.3:a:apache:http_server:2.0.28:beta:*****:
cpe:2.3:a:apache:http_server:2.0.32:*****:
cpe:2.3:a:apache:http_server:2.0.32:beta:*****:
cpe:2.3:a:apache:http_server:2.0.34:beta:*****:
cpe:2.3:a:apache:http_server:2.0.35:*****:
cpe:2.3:a:apache:http_server:2.0.36:*****:
cpe:2.3:a:apache:http_server:2.0.37:*****:
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:2.0.43:*****:
cpe:2.3:a:apache:http_server:2.0.44:*****:
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:2.0.63:*****:

cpe:2.3:a:apache:http_server:2.0.64:*****:

cpe:2.3:a:apache:http_server:2.0.9:*****:

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:2.2.11:*****:

cpe:2.3:a:apache:http_server:2.2.12:*****:

cpe:2.3:a:apache:http_server:2.2.13:*****:

cpe:2.3:a:apache:http_server:2.2.14:*****:

cpe:2.3:a:apache:http_server:2.2.15:*****:

cpe:2.3:a:apache:http_server:2.2.16:*****:

cpe:2.3:a:apache:http_server:2.2.18:*****:

cpe:2.3:a:apache:http_server:2.2.19:*****:

cpe:2.3:a:apache:http_server:2.2.2:*****:

cpe:2.3:a:apache:http_server:2.2.20:*****:

cpe:2.3:a:apache:http_server:2.2.21:*****:

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:2.2.8:*****:

cpe:2.3:a:apache:http_server:2.2.9:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 /r/debian	Help with checking changelog history on installed applications.	2016-12-14 09:17:33
← 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](#)