



CVE-2009-3095

Published on: 09/08/2009 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:04:00 AM UTC

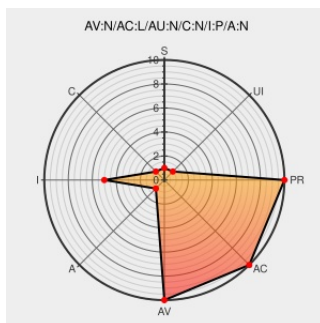
CVE-2009-3095

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The `mod_proxy_ftp` module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11.

CVE-2009-3095 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

'[security bulletin] HPSBOV02506
SSRT090244 rev.1 - HP Secure Web
Server for OpenVMS (based on
Apache' - MARC

[Third Party Advisory](#)
[marc.info](#)
[text/html](#)

[HP SSRT090244](#)

Debian -- Security Information -- DSA-
1934-1 apache2

[Third Party Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-1934](#)

Pony Mail!

[lists.apache.org](#)
[text/html](#)

[MLIST \[httpd-cvs\] 20210330 svn commit: r1073149 \[7/13\] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/](#)

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] 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
Pony Mail!	Mailing List Vendor Advisory 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
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com text/html	 BUGTRAQ 20091124 rPSA-2009-0155-1 httpd mod_ssl
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
[SECURITY] Fedora 12 Update: httpd-2.2.14-1.fc12	Third Party Advisory www.redhat.com text/html	 FEDORA FEDORA-2009-12606
'[security bulletin] HPSBMU02753 SSRT100782 rev.1 - HP Business Availability Center (BAC) Running Apa' - MARC	Third Party Advisory marc.info text/html	 HP SSRT100782
Advisories:rPSA-2009-0155 - rPath Wiki	Broken Link web.archive.org text/html Inactive Link Not Archived	 CONFIRM wiki.rpath.com/Advisories:rPSA-2009-0155
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:9363
Pony Mail!	Mailing List Vendor Advisory 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
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [6/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
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/
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073140 [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

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: r1888194 [6/13] - /http/site/trunk/content/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!	Mailing List Vendor Advisory 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	Third Party Advisory oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:8662
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!	Mailing List Vendor Advisory 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] 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
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
SUSE update for apache2 and libapr1 - Secunia Advisories - Vulnerability Information - Secunia.com	Third Party Advisory web.archive.org text/html	 SECUNIA 37152
'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC	Third Party Advisory marc.info text/html	 HP SSRT090208
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	Mailing List Third Party Advisory lists.apple.com text/html	 APPLE APPLE-SA-2010-03-29-1
Bug 522209 – CVE-2009-3095 httpd: mod_proxy_ftp FTP command injection via Authorization HTTP header	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=522209
Pony Mail!	Mailing List	 MLIST [httpd-cvs] 20200401 svn commit: r1058587 [2/4] - in

	Vendor Advisory lists.apache.org text/html	/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
[security-announce] SUSE Security Announcement: Apache and libapr (SUSE-	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2009:050
Pony Mail!	Mailing List Vendor Advisory 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
'[security bulletin] HPSBUX02531 SSRT100108 rev.1 - HP-UX Running Apache-based Web Server, Remote Den' - MARC	Third Party Advisory marc.info text/html	 HP HPSBUX02531
[SECURITY] Fedora 10 Update: httpd-2.2.14-1.fc10	Third Party Advisory www.redhat.com text/html	 FEDORA FEDORA-2009-12604
404 Not Found	Broken Link intevydis.com text/html Inactive Link Not Archived	 MISC intevydis.com/vd-list.shtml
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	Third Party Advisory support.apple.com text/html	 CONFIRM support.apple.com/kb/HT4077
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
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	All
Operating System	Apple	Mac Os X	All	All	All	All

Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Fedoraproject	Fedora	10	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Fedoraproject	Fedora	10	All	All	All
Operating System	Fedoraproject	Fedora	12	All	All	All
Operating System	Opensuse	Opensuse	10.3	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Opensuse	Opensuse	10.3	All	All	All
Operating System	Opensuse	Opensuse	11.0	All	All	All
Operating System	Opensuse	Opensuse	11.1	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp2	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp2	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All

Operating System	Suse	Linux Enterprise Server	11	-	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
cpe:2.3:a:apache:http_server:*.*.*.*.*.*.*.*:						
cpe:2.3:a:apache:http_server:*.*.*.*.*.*.*.*:						
cpe:2.3:o:apple:mac_os_x:*.*.*.*.*.*.*.*:						
cpe:2.3:o:apple:mac_os_x:*.*.*.*.*.*.*.*:						
cpe:2.3:o:debian:debian_linux:4.0:*.*.*.*.*.*.*.*:						
cpe:2.3:o:debian:debian_linux:4.0:*.*.*.*.*.*.*.*:						
cpe:2.3:o:fedoraproject:fedora:10:*.*.*.*.*.*.*.*:						
cpe:2.3:o:fedoraproject:fedora:12:*.*.*.*.*.*.*.*:						
cpe:2.3:o:fedoraproject:fedora:10:*.*.*.*.*.*.*.*:						
cpe:2.3:o:fedoraproject:fedora:12:*.*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:opensuse:10.3:*.*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:opensuse:11.0:*.*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:opensuse:11.1:*.*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:opensuse:10.3:*.*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:opensuse:11.0:*.*.*.*.*.*.*.*:						
cpe:2.3:o:opensuse:opensuse:11.1:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp2:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp2:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_server:10:sp2:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_server:11:-:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_server:9:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_server:10:sp2:*.*.*.*.*.*.*.*:						
cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*.*.*.*.*.*.*.*:						

cpe:2.3:o:suse:linux_enterprise_server:11:-:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:9:-:*:*:*:*:*:

[← 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](#)