

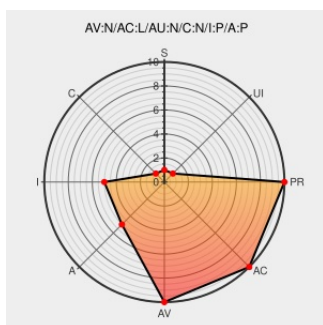


CVE-2003-0192

Published on: 07/10/2003 12:00:00 AM UTC

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

CVE-2003-0192

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

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

Apache 2 before 2.0.47, and certain versions of mod_ssl for Apache 1.3, do not properly handle "certain sequences of per-directory renegotiations and the SSLCipherSuite directive being used to upgrade from a weak ciphersuite to a strong one," which could cause Apache to use the weak ciphersuite.

CVE-2003-0192 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

[ftp.sco.com](#)
[text/plain](#)

[SCO SCOSA-2004.6](#)

Pony Mail!

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

MLIST [httpd-cvs] 20210330 svn commit: r1073139 [2/13] - in /websites/staging/httpd/trunk/content: ./ security/json/

redhat.com | Red Hat
Support

[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2003:243](#)

Pony Mail!

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

MLIST [httpd-cvs] 20210330 svn commit: r1073140 [2/4] - 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](#)

MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in

	text/html	/websites/staging/httpd/trunk/content: ./ security/
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
redhat.com Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2003:240
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1888194 [2/13] - /httpd/site/trunk/content/security/json/
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:244
No Description Provided	marc.info text/html	 BUGTRAQ 20030709 [ANNOUNCE][SECURITY] Apache 2.0.47 released
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:169
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073149 [3/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
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
Mandriva Security Advisories	www.mandriva.com text/html	 MANDRAKE MDKSA-2003:075
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
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] 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] 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

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	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	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	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	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
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:2.0.32:*:*:*:*:*.*						

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:*****:
cpe:2.3:a:apache:http_server:2.0.28:*****:
cpe:2.3:a:apache:http_server:2.0.32:*****:
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:*****:

© [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](#)