



CVE-2003-0542

Published on: 10/30/2003 12:00:00 AM UTC

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

CVE-2003-0542

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

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

Multiple stack-based buffer overflows in (1) mod_alias and (2) mod_rewrite for Apache before 1.3.29 allow attackers to create configuration files to cause a denial of service (crash) or execute arbitrary code via a regular expression with more than 9 captures.

CVE-2003-0542 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Secunia - Advisories - Red Hat update for httpd

[web.archive.org](#)
[text/html](#)

[X](#) SECUNIA 10463

redhat.com | Red Hat Support

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

[REDHAT](#) RHSA-2003:405

Pony Mail!

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

[MLIST](#) [httpd-cvs] 20210606 svn commit: r1075470 [1/4] - 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

#101841: Updated Solaris 8 Patches for Apache Security Vulnerabilities

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[SUNALERT](#) 101841

Apple security updates

[web.archive.org](#)

[CONFIRM](#) docs.info.apple.com/article.html?artnum=61798

	text/html Inactive Link Not Archived	
Apple - Lists.apple.com	lists.apple.com text/html	 CONFIRM lists.apple.com/mhonarc/security-announce/msg00045.html
Secunia - Advisories - Gentoo update for apache	web.archive.org text/html	 SECUNIA 10260
VU#549142 - Apache mod_alias vulnerable to buffer overflow via crafted regular expression	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#549142
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:360
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF apache-modalias-modrewrite-bo(13400)
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073140 [1/4] - 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
	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/
APPLE-SA-2004-01-26 Security Update 2004-01-26	lists.apple.com text/html	 APPLE APPLE-SA-2004-01-26
VU#434566 - Apache mod_rewrite vulnerable to buffer overflow via crafted regular expression	US Government Resource www.kb.cert.org text/html	 CERT-VN VU#434566
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: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/
'GLSA: apache (200310-04)' - MARC	marc.info text/html	 BUGTRAQ 20031031 GLSA: apache (200310-04)
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:9458
'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC	marc.info text/html	 HP SSRT090208
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:863
Secunia - Advisories - OpenBSD update for httpd	web.archive.org text/html	 SECUNIA 10112
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

Secunia - Advisories - HP-UX Apache Various Module Vulnerabilities	web.archive.org text/html	 SECUNIA 10264
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:816
Secunia - Advisories - Fedora update for httpd	web.archive.org text/html	 SECUNIA 10593
Secunia - Advisories - OpenPKG update for Apache	web.archive.org text/html	 SECUNIA 10098
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:320
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1888194 [2/13] - /httpd/site/trunk/content/security/json/
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20031203-01-U
Secunia - Advisories - HP-UX update for VirtualVault	web.archive.org text/html	 SECUNIA 10580
Pony Mail!	lists.apache.org text/html	 MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
Apache Web Server Multiple Module Local Buffer Overflow Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	 BID 8911
MandrakeSecure: MandrakeSoft Security Advisory MDKSA-2003:103 : apache	web.archive.org text/html Inactive Link Not Archived	 MANDRAKE MDKSA-2003:103
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
Secunia - Advisories - Conectiva update for Apache	web.archive.org text/html	 SECUNIA 10153
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:3799
Multiple Apple Mac OS X Operating System Component Vulnerabilities	cve.report (archive) text/html	 BID 9504
SecurityFocus HOME Advisories: SSRT3663 Apache HTTP Server mod_cgid, mod_alias, m	web.archive.org text/html Inactive Link Not Archived	 HP HPSBUX0311-301
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20031028 [OpenPKG-SA-2003.046] OpenPKG Security Advisory (apache)
redhat.com Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2004:015
No Description Provided	sunsolve.sun.com	 SUNALERT 101444

Inactive Link Not Archived

Secunia - Advisories - Apache Vulnerabilities in Various Modules

web.archive.org
text/html

X SECUNIA 10096

Secunia - Advisories - Immunix update for Apache

web.archive.org
text/html

X SECUNIA 10102

No Description Provided

patches.sgi.com

SGI 20040202-01-U

Inactive Link Not Archived

Download - The Apache HTTP Server Project

httpd.apache.org
text/html

CONFIRM httpd.apache.org/dist/httpd/Announcement2.html

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

Repository / Oval Repository

oval.cisecurity.org
text/html

OVAL oval:org.mitre.oval:def:864

Secunia - Advisories - Gentoo update for apache2

web.archive.org
text/html

X SECUNIA 10114

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	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	1.3.12	All	All	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.17	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	1.3.20	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	1.3.3	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.6	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	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	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	1.3.12	All	All	All
Application	Apache	Http Server	1.3.14	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	1.3.20	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	1.3.3	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.6	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	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
cpe:2.3:a:apache:http_server:1.3:*:*:*:*:*:						
cpe:2.3:a:apache:http_server:1.3.1:*:*:*:*:*:						
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:1.3.14:*****:
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:1.3.20:*****:
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:1.3.3:*****:
cpe:2.3:a:apache:http_server:1.3.4:*****:
cpe:2.3:a:apache:http_server:1.3.6:*****:
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:2.0.32:*****:
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:2.0.47:*****:
cpe:2.3:a:apache:http_server:1.3:*****:
cpe:2.3:a:apache:http_server:1.3.1:*****:
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:1.3.14:*****:
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:1.3.20:*****:
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:1.3.3:*****:
cpe:2.3:a:apache:http_server:1.3.4:*****:
cpe:2.3:a:apache:http_server:1.3.6:*****:
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:2.0.32:*****:
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:2.0.47:*****:

← Previous ID

Next ID→