

Apache News Online: Apache HTTP

Table of contents

14 June 2008 - Apache HTTP Server 2.2.9 Released.....	3
19 January 2008 - Apache HTTP Server 2.2.8 (2.0.63, 1.3.41) Released.....	4
19 January 2008 - Apache HTTP Server 2.0.63 (2.2.8, 1.3.41) Released.....	6
19 January 2008 - Apache HTTP Server 1.3.41 (2.2.8, 2.0.63) Released.....	8
16 February 2007 - Mod_python 3.3.1 released.....	10
10 January 2007 - Apache HTTP Server 2.2.4 Released.....	11
26 December 2006 - Mod_python 3.3.0b (Beta) Now Available.....	12
10 August 2006 - libapreq2-2.08 Released.....	13
07 August 2006 - Mod_python 3.2.10.....	13
28 July 2006 - Apache HTTP Server 2.2.3 Released.....	14
01 May 2006 - Apache HTTP Server 2.2.2 Released.....	16
02 December 2005 - Apache HTTP Server 2.2.0 Released.....	17
23 November 2005 - Mod_python 3.2.5 Beta Now Available.....	18
07 November 2005 - Apache HTTP Server 2.1.9-beta Now Available.....	18
18 October 2005 - Apache HTTP Server 1.3.34 Released.....	18
14 October 2005 - Apache HTTP Server 2.0.55 Released.....	21
02 October 2005 - Apache HTTP Server 2.1.8-beta Now Available.....	23
12 September 2005 - Apache HTTP Server 2.1.7-beta Now Available.....	23
05 May 2005 - Apache HTTP Server Request Library 2.05-dev Released.....	24
17 April 2005 - Apache HTTP Server 2.0.54 Released.....	25
13 February 2005 - Mod_python 3.1.4 and 2.7.11 (Security Release).....	26
08 February 2005 - Apache HTTP Sever 2.0.53 Released.....	27
28 September 2004 - Apache HTTP Server 2.0.52 Released.....	28
15 September 2004 - Apache HTTP Server 2.0.51 Released.....	29

30 August 2004 - Apache HTTP Server Request Library 2.04-dev Released.....	30
30 June 2004 - Apache HTTP Server 2.0.50 Released.....	31
11 May 2004 - Apache HTTP Server 1.3.31 Released.....	32
11 May 2004 - Press Release: Apache HTTP Server Technical Leadership.....	33
19 March 2004 - Apache HTTP Server 2.0.49 Released.....	34
03 March 2004 - Mod_python 3.1.3 Released.....	35
22 January 2004 - Mod_python 2.7.10 Released.....	35
28 November 2003 - Mod_python 3.0.4 and 2.7.9 Released.....	36
29 October 2003 - Apache HTTP Server 1.3.29 Released.....	36
29 October 2003 - Apache HTTP Server 2.0.48 Released.....	37
27 October 2003 - Mod_python 3.1.2 Beta Released.....	38
18 Jul 2003 - Apache HTTP Server 1.3.28 released.....	38
09 Jul 2003 - Apache Http Server 2.0.47 released.....	39
28 May 2003 - Apache 2.0.46 released.....	39
02 April 2003 - Apache 2.0.45 Released.....	40
17 March 2003 - Mod_python 3.0.3 Released.....	40
28 November 2002 - Mod_python 3.0.1 Released.....	41
13 September 2002 - Mod_Python donated to ASF.....	41

14 June 2008 - Apache HTTP Server 2.2.9 Released

[The Apache Software Foundation](#) and [the Apache HTTP Server Project](#) are pleased to announce the release of version 2.2.9 of the Apache HTTP Server ("Apache"). This version of Apache is principally a bug and security fix release. The following potential security flaws are addressed:

- CVE-2008-2364 (cve.mitre.org) -- mod_proxy_http: Better handling of excessive interim responses from origin server to prevent potential denial of service and high memory usage. Reported by Ryujiro Shibuya.
- CVE-2007-6420 (cve.mitre.org) -- mod_proxy_balancer: Prevent CSRF attacks against the balancer-manager interface.

We consider this release to be the best version of Apache available, and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.2.9 is available for download from:

<http://httpd.apache.org/download.cgi>

Apache 2.2 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced since 2.0 please see:

http://httpd.apache.org/docs/2.2/new_features_2_2.html

Please see the CHANGES_2.2 file, linked from the download page, for a full list of changes. A condensed list, CHANGES_2.2.9 provides the complete list of changes since 2.2.8. A summary of security vulnerabilities which were addressed in the previous 2.2.8 and earlier releases is available:

http://httpd.apache.org/security/vulnerabilities_22.html

Apache HTTP Server 1.3.41 and 2.0.63 legacy releases are also currently available. See the appropriate CHANGES from the url above. See the corresponding CHANGES files linked from the download page. The Apache HTTP Project developers strongly encourage all users to migrate to Apache 2.2, as only limited maintenance is performed on these legacy versions.

This release includes [the Apache Portable Runtime](#) (APR) version 1.3.0 bundled with the tar and zip distributions. The APR libraries libapr and libaprutil (and on Win32, libapricnv) must all be updated to ensure binary compatibility and address many known platform bugs.

This release builds on and extends the Apache 2.0 API. Modules written for Apache 2.0 will need to be recompiled in order to run with Apache 2.2, and require minimal or no source code changes.

<http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/VERSIONING>

When upgrading or installing this version of Apache, please bear in mind that if you intend to use Apache with one of the threaded MPMs (other than the Prefork MPM), you must ensure that any modules you will be using (and the libraries they depend on) are thread-safe.

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2008-06-14T00:21:57](#)

19 January 2008 - Apache HTTP Server 2.2.8 (2.0.63, 1.3.41) Released

Apache HTTP Server 2.2.8 Released

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the release of version 2.2.8 of the Apache HTTP Server ("Apache"). This version of Apache is principally a bug and security fix release. The following potential security flaws are addressed:

- CVE-2007-6421 (cve.mitre.org)
mod_proxy_balancer: Correctly escape the worker route and the worker redirect string in the HTML output of the balancer manager. Reported by SecurityReason.

A flaw was found in the mod_proxy_balancer module. On sites where mod_proxy_balancer is enabled, a cross-site scripting attack against an authorized user is possible.

- CVE-2007-6422 (cve.mitre.org)
Prevent crash in balancer manager if invalid balancer name is passed as parameter. Reported by SecurityReason.

A flaw was found in the mod_proxy_balancer module. On sites where mod_proxy_balancer is enabled, an authorized user could send a carefully crafted request that would cause the Apache child process handling that request to crash. This could lead to a denial of service if using a threaded Multi-Processing Module.

- CVE-2007-6388 (cve.mitre.org)

mod_status: Ensure refresh parameter is numeric to prevent a possible XSS attack caused by redirecting to other URLs. Reported by SecurityReason.

A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.

- CVE-2007-5000 (cve.mitre.org)
mod_imagemap: Fix a cross-site scripting issue. Reported by JPCERT.

A flaw was found in the mod_imap module. On sites where mod_imap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

We consider this release to be the best version of Apache available, and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.2.8 is available for download from:

<http://httpd.apache.org/download.cgi>

Apache 2.2 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced since 2.0 please see:

http://httpd.apache.org/docs/2.2/new_features_2_2.html

Please see the CHANGES_2.2 file, linked from the download page, for a full list of changes. A condensed list, CHANGES_2.2.8 provides the complete list of changes since 2.2.6 (2.2.7 was not released). A summary of security vulnerabilities which were addressed in the previous 2.2.6 and earlier releases is available:

http://httpd.apache.org/security/vulnerabilities_22.html

Apache HTTP Server 1.3.41 and 2.0.63 legacy releases are also currently available. See the appropriate CHANGES from the url above. See the corresponding CHANGES files linked from the download page. The Apache HTTP Project developers strongly encourage all users to migrate to Apache 2.2, as only limited maintenance is performed on these legacy versions.

This release includes the Apache Portable Runtime (APR) version 1.2.12 bundled with the tar and zip distributions. The APR libraries libapr and libaprutil (and on Win32, libapriconv) must all be updated to ensure binary compatibility and address many known platform bugs.

This release builds on and extends the Apache 2.0 API. Modules written for Apache 2.0 will need to be recompiled in order to run with Apache 2.2, and require minimal or no source code changes.

<http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/VERSIONING>

When upgrading or installing this version of Apache, please bear in mind that if you intend to use Apache with one of the threaded MPMs (other than the Prefork MPM), you must ensure that any modules you will be using (and the libraries they depend on) are thread-safe.

-- The Apache Software Foundation and the Apache HTTP Server Project

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2008-01-20T00:51:27](#)

19 January 2008 - Apache HTTP Server 2.0.63 (2.2.8, 1.3.41) Released

Apache HTTP Server 2.0.63 Released

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the legacy release of version 2.0.63 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.63 as compared to 2.0.61 (2.0.62 was not released). This Announcement 2.0 document may also be available in multiple languages at:

<http://www.apache.org/dist/httpd/>

This version of Apache is principally a bug and security fix release. The following potential security flaws are addressed:

- CVE-2007-6388 (cve.mitre.org)
mod_status: Ensure refresh parameter is numeric to prevent a possible XSS attack caused by redirecting to other URLs. Reported by SecurityReason.

A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.

- CVE-2007-5000 (cve.mitre.org)
mod_imagemap: Fix a cross-site scripting issue. Reported by JPCERT.

A flaw was found in the mod_imap module. On sites where mod_imap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

Please see the CHANGES_2.0.63 file in this directory for a full list of changes for this version.

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache 2.0 available and encourage users of all prior versions to upgrade.

This release includes the Apache Portable Runtime library suite release version 0.9.17, bundled with the tar and zip distributions. These libraries; libapr, libaprutil, and on Win32, libapriconv must all be updated to ensure binary compatibility and address many known platform bugs.

Apache HTTP Server 2.0.63 is available for download from

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes. A condensed list, CHANGES_2.0.63 provides the complete list of changes since 2.0.61.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see

http://httpd.apache.org/docs/2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following: If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please refer to the documentation of these modules and libraries to obtain this information.

Apache 2.2 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced after 2.0 please see

http://httpd.apache.org/docs/2.2/new_features_2_2.html

We consider Apache 2.2 to be the best available version at the time of this release. We offer Apache 2.0.63 as the best legacy version of Apache 2.0 available. Users should first consider upgrading to the current release of Apache 2.2 instead.

-- The Apache Software Foundation and The Apache HTTP Server Project

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2008-01-20T00:43:41](#)

19 January 2008 - Apache HTTP Server 1.3.41 (2.2.8, 2.0.63) Released

Apache HTTP Server 1.3.41 Released

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the release of version 1.3.41 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 1.3.41 as compared to 1.3.39 (1.3.40 was not released).

This version of Apache is principally a bug and security fix release. The following potential security flaws are addressed:

- CVE-2007-6388 ([cve.mitre.org](#))
mod_status: Ensure refresh parameter is numeric to prevent a possible XSS attack caused by redirecting to other URLs. Reported by SecurityReason.

A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.

- CVE-2007-5000 ([cve.mitre.org](#))
mod_imap: Fix cross-site scripting issue. Reported by JPCERT.

A flaw was found in the mod_imap module. On sites where mod_imap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

- CVE-2007-3847 ([cve.mitre.org](#))
mod_proxy: Prevent reading past the end of a buffer when parsing date-related headers. PR 41144. With Apache 1.3, the denial of service vulnerability applies only to the Windows and NetWare platforms.

Please see the CHANGES_1.3.41 file in this directory for a full list of changes for this version.

Apache 1.3.41 is the current stable release of the Apache 1.3 family. We strongly recommend that users of all earlier versions, including 1.3 family release, upgrade to to the current 2.2 version as soon as possible.

We recommend Apache 1.3.41 version for users who require a third party module that is not yet available as an Apache 2.x module. Modules compiled for Apache 2.x are not compatible with Apache 1.3, and modules compiled for Apache 1.3 are not compatible with Apache 2.x.

Apache 1.3.41 is available for download from

<http://httpd.apache.org/download.cgi>

This service utilizes the network of mirrors listed at:

<http://www.apache.org/mirrors/>

Binary distributions may be available for your specific platform from

<http://www.apache.org/dist/httpd/binaries/>

Binaries distributed by the Apache HTTP Server Project are provided as a courtesy by individual project contributors. The project makes no commitment to release the Apache HTTP Server in binary form for any particular platform, nor on any particular schedule.

IMPORTANT NOTE FOR APACHE USERS: Apache 1.3 was designed for Unix OS variants. While the ports to non-Unix platforms (such as Win32, Netware or OS2) will function for some applications, Apache 1.3 is not designed for these platforms. Apache 2 was designed from the ground up for security, stability, or performance issues across all modern operating systems. Users of any non-Unix ports are strongly cautioned to move to Apache 2.

The Apache project no longer distributes non-Unix platform binaries from the main download pages for Apache 1.3. If absolutely necessary, a binary may be available at <http://archive.apache.org/dist/httpd/>.

Apache is the most popular web server in the known universe; about 2/3 of the servers on the Internet run Apache HTTP Server, or one of its variants.

Bugfixes addressed in 1.3.41 are:

More efficient implementation of the CVE-2007-3304 PID table patch. This fixes issues with excessive memory usage by the parent process if long-running and with a high number of child process forks during that timeframe. Also fixes bogus "Bad pid" errors.

-- The Apache Software Foundation and The Apache HTTP Server Project

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2008-01-20T00:34:43](#)

16 February 2007 - Mod_python 3.3.1 released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the 3.3.1 release of mod_python. Mod_python 3.3.1 is considered a stable release, suitable for production use.

Mod_python is an Apache HTTP Server module that embeds the Python language interpreter within the server. With mod_python you can write web-based applications in Python that will run many times faster than traditional CGI and will have access to advanced features such as ability to maintain objects between requests, access to httpd internals, content filters and connection handlers.

The 3.3.1 release has many new features, feature enhancements, fixed bugs and other improvements over the previous version. See Appendix A of mod_python documentation for more details.

Mod_python 3.3.1 is released under the new [Apache License version 2.0](#).

Mod_python 3.3.1 is available for download from:

<http://httpd.apache.org/modules/python-download.cgi>

More information about mod_python is available at:

<http://httpd.apache.org/modules/>

Many thanks to everyone who contributed to and helped test this release, without your help it would not be possible.

Regards,

-- **The Apache Mod_python team**

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2007-02-16T00:00:49](#)

10 January 2007 - Apache HTTP Server 2.2.4 Released

Apache HTTP Server 2.2.4 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the [release](#) of version 2.2.4 of the Apache HTTP Server ("Apache"). This version of Apache is principally a bugfix release.

We consider this release to be the best version of Apache available, and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.2.4 is available for download from:

<http://httpd.apache.org/download.cgi>

Apache 2.2 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced since 2.0 please see:

http://httpd.apache.org/docs/2.2/new_features_2_2.html

Please see the CHANGES_2.2 file, linked from the download page, for a full list of changes. A summary of security vulnerabilities which were addressed in the previous 2.2.3 and earlier releases is available:

http://httpd.apache.org/security/vulnerabilities_22.html

Apache HTTP Server 1.3.37 and 2.0.59 legacy releases are also currently available. See the appropriate CHANGES from the url above. See the corresponding CHANGES files linked from the download page. The Apache HTTP Project developers strongly encourage all users to migrate to Apache 2.2, as only limited maintenance is performed on these legacy versions.

This release includes the Apache Portable Runtime (APR) version 1.2.8 bundled with the tar and zip distributions. The APR libraries libapr and libaprutil (and on Win32, libapriconv) must all be updated to ensure binary compatibility and address many known platform bugs.

This release builds on and extends the Apache 2.0 API. Modules written for Apache 2.0 will need to be recompiled in order to run with Apache 2.2, and require minimal or no source code changes.

<http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/VERSIONING>

When upgrading or installing this version of Apache, please bear in mind that if you intend to use Apache with one of the threaded MPMs (other than the Prefork MPM), you must ensure that any modules you will be using (and the libraries they depend on) are thread-safe.

[-- The Apache HTTP Server Project](#)

[-- The Apache Software Foundation](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2007-01-10T22:56:27](#)

26 December 2006 - Mod_python 3.3.0b (Beta) Now Available

The Apache mod_python team is pleased to announce the 3.3.0b (Beta) release of mod_python.

Version 3.3.0b of mod_python features several new functions and attributes providing better access to apache internals, as well as many bug fixes and various performance and security improvements. A detailed description of the changes is available in Appendix A of the mod_python manual, also available here

http://www.modpython.org/live/mod_python-3.3.0b/doc-html/app-changes-from-3.2.10.html

Beta releases are NOT considered stable and usually contain bugs.

This release is intended to solicit widespread testing of the code. We strongly recommend that you try out your existing applications and experiment with new features in a non-production environment using this version and report any problems you may encounter so that they can be addressed before the final release.

Preferred method of reporting problems is the mod_python user list mod_python@modpython.org.

Mod_python 3.3.0b is available for download from:

<http://httpd.apache.org/modules/python-download.cgi>

For more information about mod_python visit <http://www.modpython.org/>

-- The Apache mod_python team

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2006-12-26T23:49:22](#)

10 August 2006 - libapreq2-2.08 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the 2.08 release of libapreq2. This Announcement notes significant changes introduced by this release.

libapreq2-2.08 is released under the Apache License version 2.0. It is now available through the ASF mirrors

<http://httpd.apache.org/apreq/download.cgi>

and has entered the CPAN as

- file: \$CPAN/authors/id/J/JO/JOESUF/libapreq2-2.08.tar.gz
- size: 847527 bytes
- md5: 9fb3deec448f74c455d4ffc13846ea9f

libapreq2 is an [APR](#)-based shared library used for parsing HTTP cookies, query-strings and POST data. This package provides

1. version 2.6.0 of the libapreq2 library,
2. mod_apreq2, a filter module necessary for using libapreq2 within the Apache HTTP Server,
3. the Apache2::Request, Apache2::Cookie, and Apache2::Upload perl modules for using libapreq2 with [mod_perl2](#).

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2006-08-10T16:06:37](#)

07 August 2006 - Mod_python 3.2.10

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the 3.2.10 release of mod_python. Mod_python 3.2.10 is considered a stable release, suitable for production use. Mod_python is an Apache HTTP Server module that embeds the Python language interpreter within the server. With mod_python you can write web-based applications in Python that will run many times faster than traditional CGI and will have access to advanced features such as

ability to maintain objects between requests, access to httpd internals, content filters and connection handlers. The 3.2.10 release has many new features, feature enhancements, fixed bugs and other improvements over the previous version. 3.2.10 now works with Apache HTTP Server 2.2. See Appendix A of mod_python documentation for a complete list. Mod_python 3.2.10 is released under Apache License version 2.0. Mod_python 3.2.10 is available for download from: <http://httpd.apache.org/modules/python-download.cgi> More information about mod_python is available at: <http://httpd.apache.org/modules/> Many thanks to Jim Gallacher, Graham Dumbleton, Nicolas Lehen and everyone else who contributed to and helped test this release, without your help it would not be possible ---- -- The Apache HTTP Server Project...

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2006-08-07T17:48:03](#)

28 July 2006 - Apache HTTP Server 2.2.3 Released

Apache HTTP Server 2.2.3 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the [release](#) of version 2.2.3 of the Apache HTTP Server ("Apache").

This version of Apache is principally a bug and security fix release. The following potential security flaws are addressed;

- CVE-2006-3747: An off-by-one flaw exists in the Rewrite module, mod_rewrite, as shipped with Apache 1.3 since 1.3.28, 2.0 since 2.0.46, and 2.2 since 2.2.0.

Depending on the manner in which Apache HTTP Server was compiled, this software defect may result in a vulnerability which, in combination with certain types of Rewrite rules in the web server configuration files, could be triggered remotely. For vulnerable builds, the nature of the vulnerability can be denial of service (crashing of web server processes) or potentially allow arbitrary code execution. This issue has been rated as having important security impact by the Apache HTTP Server Security Team.

This flaw does not affect a default installation of Apache HTTP Server. Users who do not use, or have not enabled, the Rewrite module mod_rewrite are not affected by this issue. This issue only affects installations using a Rewrite rule with the following characteristics:

- The RewriteRule allows the attacker to control the initial part of the rewritten URL (for

example if the substitution URL starts with \$1)

- The RewriteRule flags do NOT include any of the following flags: Forbidden (F), Gone (G), or NoEscape (NE).

Please note that ability to exploit this issue is dependent on the stack layout for a particular compiled version of mod_rewrite. If the compiler used to compile Apache HTTP Server has added padding to the stack immediately after the buffer being overwritten, it will not be possible to exploit this issue, and Apache HTTP Server will continue operating normally.

The Apache HTTP Server project recommends that all users who have built Apache from source apply the patch or upgrade to the latest level and rebuild. Providers of Apache-based web servers in pre-compiled form will be able to determine if this vulnerability applies to their builds. That determination has no bearing on any other builds of Apache HTTP Server, and Apache HTTP Server users are urged to exercise caution and apply patches or upgrade unless they have specific instructions from the provider of their web server. Statements from vendors can be obtained from the US-CERT vulnerability note for this issue at:

<http://www.kb.cert.org/vuls/id/395412>

The Apache HTTP Server project thanks Mark Dowd of McAfee Avert Labs for the responsible reporting of this vulnerability.

We consider this release to be the best version of Apache available, and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.2.3 is available for download from:

<http://httpd.apache.org/download.cgi>

Apache 2.2 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced since 2.0 please see:

http://httpd.apache.org/docs/2.2/new_features_2_2.html

Please see the CHANGES_2.2 file, linked from the download page, for a full list of changes.

Apache HTTP Server 1.3.37 and 2.0.59 legacy releases are also available with this security fix. See the appropriate CHANGES from the url above. The Apache HTTP Project developers strongly encourage all users to migrate to Apache 2.2, as only limited maintenance is performed on these legacy versions.

This release includes the Apache Portable Runtime (APR) version 1.2.7 bundled with the tar and zip distributions. The APR libraries libapr, libaprutil, and (on Win32) libapriconv must all be updated to ensure binary compatibility and address many known platform bugs.

This release builds on and extends the Apache 2.0 API. Modules written for Apache 2.0 will need to be recompiled in order to run with Apache 2.2, but no substantial reworking should be necessary.

<http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/VERSIONING>

When upgrading or installing this version of Apache, please bear in mind that if you intend to use Apache with one of the threaded MPMs, you must ensure that any modules you will be using (and the libraries they depend on) are thread-safe.

[-- The Apache HTTP Server Project](#)

[-- The Apache Software Foundation](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2006-07-28T20:58:10](#)

01 May 2006 - Apache HTTP Server 2.2.2 Released

Apache HTTP Server 2.2.2 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of version 2.2.2 of the Apache HTTP Server ("Apache").

We consider this release to be the best version of Apache available, and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.2.2 is available for download from:

<http://httpd.apache.org/download.cgi>

Apache 2.2 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced since 2.0 please see:

http://httpd.apache.org/docs/2.2/new_features_2_2.html

Please see the CHANGES_2.2 file, linked from the download page, for a full list of changes.

Apache HTTP Server 1.3.35 and 2.0.58 legacy releases are also available with minor bugfixes. See the appropriate CHANGES from the url above. The Apache HTTP Project developers strongly encourages all users to migrate to Apache 2.2, as only limited maintenance is performed on these legacy versions.

This release includes the [Apache Portable Runtime \(APR\)](#) version 1.2.7 bundled with the tar and zip distributions. The APR libraries libapr, libaprutil, and (on Win32) libapriconv must all be updated to ensure binary compatibility and address many known platform bugs.

This release has been through extensive testing, including live at some of the world's busiest sites, and is now considered stable. This means that modules and applications developed for Apache 2.2.2 will be both source- and binary-compatible with future 2.2.x releases. This release builds on and extends the Apache 2.0 API. Modules written for Apache 2.0 will need to be recompiled in order to run with Apache 2.2, but no substantial reworking should be necessary.

<http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/VERSIONING>

When upgrading or installing this version of Apache, please bear in mind that if you intend to use Apache with one of the threaded MPMs, you must ensure that any modules you will be using (and the libraries they depend on) are thread-safe.

[-- The Apache Software Foundation](#)

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2006-05-01T05:46:21](#)

02 December 2005 - Apache HTTP Server 2.2.0 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.2.0 of the Apache HTTP Server ("Apache"). -- [\(read more\)](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-12-02T00:08:26](#)

23 November 2005 - Mod_python 3.2.5 Beta Now Available

The Apache mod_python team has announced the general availability of mod_python 3.2.5 Beta. -- [\(read more\)](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-11-24T14:01:37](#)

07 November 2005 - Apache HTTP Server 2.1.9-beta Now Available

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.1.9-beta of the Apache HTTP Server ("Apache"). This beta release should not be presumed to be compatible with binaries built against any prior or future version.

Apache HTTP Server 2.1.9-beta is available for download from:

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.1 file, linked from the above page, for a full list of changes.

Apache 2.1 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced after 2.0 please see:

http://httpd.apache.org/docs/2.1/new_features_2_2.html

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-11-07T09:28:10](#)

18 October 2005 - Apache HTTP Server 1.3.34 Released

[The Apache Software Foundation](#) and [the Apache HTTP Server Project](#) are pleased to announce the release of version 1.3.34 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 1.3.34 as compared to 1.3.33. This Announcement1.3 document may also be available in multiple languages at:

<http://www.apache.org/dist/httpd/>

This version of Apache is principally a bug and security fix release. A partial summary of the bug fixes is given at the end of this document. A full listing of changes can be found in the CHANGES file. Of particular note is that 1.3.34 addresses and fixes 2 potential security issues:

- If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks.
- Added TraceEnable [on|off|extended] per-server directive to alter the behavior of the TRACE method.

We consider Apache 1.3.34 to be the best version of Apache 1.3 available and we strongly recommend that users of older versions, especially of the 1.1.x and 1.2.x family, upgrade as soon as possible. No further releases will be made in the 1.2.x family.

Apache 1.3.34 is available for download from
<http://httpd.apache.org/download.cgi>

Binary distributions are available from
<http://www.apache.org/dist/httpd/binaries/>

This service utilizes the network of mirrors listed at:
<http://www.apache.org/mirrors/>

Please see the CHANGES_1.3 file in the same directory for a full list of changes.

As of Apache 1.3.12 binary distributions contain all standard Apache modules as shared objects (if supported by the platform) and include full source code. Installation is easily done by executing the included install script. See the README.bindist and INSTALL.bindist files for a complete explanation. Please note that the binary distributions are only provided for your convenience and current distributions for specific platforms are not always available. Win32 binary distributions are based on the Microsoft Installer (.MSI) technology. While development continues to make this installation method more robust, questions should be directed to the news:comp.infosystems.www.servers.ms-windows newsgroup.

For an overview of new features introduced after 1.2 please see
http://httpd.apache.org/docs/new_features_1_3.html

In general, Apache 1.3 offers several substantial improvements over version 1.2, including better performance, reliability and a wider range of supported platforms, including Windows 95/98 and NT (which fall under the "Win32" label), OS2, Netware, and TPE threaded platforms.

IMPORTANT NOTE FOR APACHE USERS: Apache 1.3 was designed for Unix OS variants. While the ports to non-Unix platforms (such as Win32, Netware or OS2) are of an acceptable quality, Apache 1.3 is not optimized for these platforms. Security,

stability, or performance issues on these non-Unix ports do not generally apply to the Unix version, due to software's Unix origin.

Apache 2.0 has been structured for multiple operating systems from its inception, by introducing the Apache Portability Library and MPM modules. Users on Unix and non-Unix platforms are strongly encouraged to move up to Apache 2.0 for better performance, stability and security on their platforms. We consider Apache 2.0.55 to be the best available version at the time of this release. We offer Apache 1.3.34 as the best legacy version of Apache 1.3 available, and strongly recommend that users who require compatibility with existing Apache 1.3 installations should upgrade as soon as possible. Users should first consider upgrading to the current release of Apache 2 instead.

Apache is the most popular web server in the known universe; over half of the servers on the Internet are running Apache or one of its variants.

Apache 1.3.34 Major changes

Security vulnerabilities

The main security vulnerabilities addressed in 1.3.34 are:

- If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks.
- Added TraceEnable [on|off|extended] per-server directive to alter the behavior of the TRACE method.

New features

New features that relate to specific platforms:

- None

Bugs fixed

The following bugs were found in Apache 1.3.33 (or earlier) and have been fixed in Apache 1.3.34:

- `hsregex`: Fix potential core dumping on 64 bit machines, such as AMD64. PR 31858.
- `mod_digest`: Fix another nonce string calculation issue.

[-- The Apache HTTP Server Project](#)

Product Info	
TLP (Top Level Project) Name	Apache HTTP Server Project
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server software product for various modern desktop and server operating systems. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.	
Product Name	Apache HTTP Server 1.x
The Apache HTTP Server is an open-source HTTP server for modern operating systems including UNIX, MS-Windows, Macintosh and Netware. Apache has been the most popular web server on the Internet since April of 1996	
Downloads	http://httpd.apache.org/download.cgi
Bug Tracking	http://httpd.apache.org/bug_report.html
License	Apache License Version 2.0

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-10-18T19:03:31](#)

14 October 2005 - Apache HTTP Server 2.0.55 Released

[The Apache Software Foundation](#) and [the Apache HTTP Server Project](#) are pleased to announce the release of version 2.0.55 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.55 as compared to 2.0.54. This Announcement2.0 document may also be available in multiple languages at:

<http://www.apache.org/dist/httpd/>

This version of Apache is principally a security release. The following potential security flaws are addressed, the first three of which address several classes of HTTP Request and Response Splitting/Spoofing attacks;

CAN-2005-2088 (cve.mitre.org)

core: If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length.

proxy_http: Correctly handle the Transfer-Encoding and Content-Length request headers. Discard the request Content-Length whenever chunked T-E is used, always passing one of either C-L or T-E chunked whenever the request includes a request body.

Unassigned

proxy_http: If a response contains both Transfer-Encoding and a Content-Length, remove the Content-Length and don't reuse the connection.

CAN-2005-2700 (cve.mitre.org)

mod_ssl: Fix a security issue where "SSLVerifyClient" was not enforced in per-location context if "SSLVerifyClient optional" was configured in the vhost configuration.

CAN-2005-2491 (cve.mitre.org)

pcre: Fix integer overflows in PCRE in quantifier parsing which could be triggered by a local user through use of a carefully crafted regex in an .htaccess file.

CAN-2005-2728 (cve.mitre.org)

Fix cases where the byterange filter would buffer responses into memory.

CAN-2005-1268 (cve.mitre.org)

mod_ssl: Fix off-by-one overflow whilst printing CRL information at "LogLevel debug" which could be triggered if configured to use a "malicious" CRL.

The Apache HTTP Project thanks all of the reporters of these issues and vulnerabilities for the responsible reporting and thorough analysis of these vulnerabilities.

This release further addresses a number of cross-platform bugs, as well as specific issues on OS/X 10.4, Win32, AIX, and across all EBCDIC platforms, and adds compatibility with OpenSSL 0.9.8.

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade.

This release includes the Apache Portable Runtime library suite release version 0.9.7, bundled with the tar and zip distributions. These libraries; libapr, libaprutil, and on Win32, libapriconv must all be updated to ensure binary compatibility and address many known platform bugs.

Apache 2.0.55 is available for download from

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see

http://httpd.apache.org/docs/2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following: If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please refer to the

documentation of these modules and libraries to obtain this information.

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-10-14T19:21:45](#)

02 October 2005 - Apache HTTP Server 2.1.8-beta Now Available

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.1.8-beta of the Apache HTTP Server ("Apache"). This beta release should not be presumed to be compatible with binaries built against any prior or future version.

Apache HTTP Server 2.1.8-beta is available for download from:

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.1 file, linked from the above page, for a full list of changes.

Apache 2.1 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced after 2.0 please see:

http://httpd.apache.org/docs-2.1/new_features_2_2.html

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-10-02T16:12:40](#)

12 September 2005 - Apache HTTP Server 2.1.7-beta Now Available

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.1.7-beta of the Apache HTTP Server ("Apache"). This beta release should not be presumed to be compatible with binaries built against any prior or future version.

Apache HTTP Server 2.1.7-beta is available for download from:

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.1 file, linked from the above page, for a full list of changes.

Known Issues

Several non-show-stopping issues were found during the 2.1.7-beta release cycle:

- mod_setenvif was missing updated documentation
- server/listen.c had problems working on AIX
- The RPM spec file was outdated.
- htcacheclean lacked support for recent changes to mod_disk_cache

A patch that fixes these issues is available at:

http://www.apache.org/dist/httpd/patches/apply_to_2.1.7/non-showstoppers.patch

In addition, mod_ldap in 2.1.7-beta does not compile on older version of Windows.

Apache 2.1 offers numerous enhancements, improvements, and performance boosts over the 2.0 codebase. For an overview of new features introduced after 2.0 please see:

http://httpd.apache.org/docs-2.1/new_features_2_2.html

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-09-12T19:01:20](#)

05 May 2005 - Apache HTTP Server Request Library 2.05-dev Released

libapreq2-2.05-dev Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the 2.05-dev release of libapreq2. This Announcement notes significant changes introduced by this release.

libapreq2-2.05-dev is released under the [Apache License version 2.0](#). It is now available through the ASF mirrors

<http://httpd.apache.org/apreq/download.cgi>

and has entered the CPAN as

file: \$CPAN/authors/id/J/JO/JOESUF/libapreq2-2.05-dev.tar.gz
size: 702625 bytes
md5: 0985e102b6d2bc9c747a56b04a85cba6

libapreq2 is an [APR](#)-based shared library used for parsing HTTP cookies, query-strings and POST data. This package provides

1. version 2.1.0 of the libapreq2 library,
2. mod_apreq2, a filter module necessary for using libapreq2 within the Apache HTTP Server,
3. the Apache2::Request, Apache2::Cookie, and Apache2::Upload perl modules for using libapreq2 with mod_perl2.

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-05-05T22:29:12](#)

17 April 2005 - Apache HTTP Server 2.0.54 Released

Apache HTTP Server 2.0.54 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.0.54 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.54 as compared to 2.0.53. The Announcement is also available in German and Japanese from:

<http://www.apache.org/dist/httpd/Announcement2.txt.de>
<http://www.apache.org/dist/httpd/Announcement2.txt.ja>

This version of Apache is principally a bug fix release.

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.0.54 is available for download from

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of

changes.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see

http://httpd.apache.org/docs-2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following:

If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these modules to obtain this information.

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-04-17T23:21:54](#)

13 February 2005 - Mod_python 3.1.4 and 2.7.11 (Security Release)

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of versions 3.1.4 and 2.7.11 of mod_python.

This release addresses a vulnerability in mod_python's publisher handler whereby a carefully crafted URL would expose objects that should not be visible, leading to an information leak. The Common Vulnerabilities and Exposures project (<http://cve.mitre.org/>) has assigned the name CAN-2005-0088 to this issue.

Users of the publisher handler are urged to upgrade as soon as possible.

There are no other changes or improvements from the previous version in this release.

At this point the new version is only available as a source code archive. Users of mod_python on Win32 platform can update their installation by simply replacing the publisher.py file with the latest version from the source code archive.

Mod_python is available for download from:

<http://httpd.apache.org/modules/python-download.cgi>

For more information about mod_python visit <http://www.modpython.org/>

Regards,

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-02-13T05:07:39](#)

08 February 2005 - Apache HTTP Sever 2.0.53 Released

[The Apache Software Foundation](#) and [the Apache HTTP Server Project](#) are pleased to announce the release of version 2.0.53 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.53 as compared to 2.0.52. The Announcement is also available in [German](#) and [Japanese](#) from: <http://www.apache.org/dist/httpd/Announcement2.html.de>
<http://www.apache.org/dist/httpd/Announcement2.html.ja>

This version of Apache is principally a bug fix release.

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade.

Apache 2.0.53 is available for download from -- <http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see -- http://httpd.apache.org/docs-2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following:

If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these modules to obtain this information.

[-- The Apache HTTP Server Project](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2005-02-08T15:32:50](#)

28 September 2004 - Apache HTTP Server 2.0.52 Released

The Apache Software Foundation and the The Apache HTTP Server Project are pleased to announce the release of version 2.0.52 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.52 as compared to 2.0.51. The Announcement is also available in German and Japanese from:

<http://www.apache.org/dist/httpd/Announcement2.html.de>

<http://www.apache.org/dist/httpd/Announcement2.html.ja>

This version of Apache is principally a bug fix release. Of particular note is that 2.0.52 addresses one new security related flaw introduced in 2.0.51:

Fix merging of the Satisfy directive, which was applied to the surrounding context and could allow access despite configured authentication. PR 31315.

[\[CAN-2004-0811\]](#)

The Apache HTTP Server Project would like to thank Rici Lake for identification and a proposed fix of this flaw.

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade.

Apache 2.0.52 is available for download from

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see

http://httpd.apache.org/docs-2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following:

If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these modules to obtain this information.

-- [Apache HTTP Server Project Team](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-09-28T13:41:04](#)

15 September 2004 - Apache HTTP Server 2.0.51 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.0.51 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.51 as compared to 2.0.50.

This version of Apache is principally a bug fix release. Of particular note is that 2.0.51 addresses five security vulnerabilities:

- An input validation issue in IPv6 literal address parsing which can result in a negative length parameter being passed to memcpy. [<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0786>]
- A buffer overflow in configuration file parsing could allow a local user to gain the privileges of a httpd child if the server can be forced to parse a carefully crafted .htaccess file. [<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0747>]
- A segfault in mod_ssl which can be triggered by a malicious remote server, if proxying to SSL servers has been configured. [<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0751>]
- A potential infinite loop in mod_ssl which could be triggered given particular timing of a connection abort. [<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0748>]
- A segfault in mod_dav_fs which can be remotely triggered by an indirect lock refresh request. [<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0809>]

The Apache HTTP Server Project would like to thank Codenomicon for supplying copies of their "HTTP Test Tool" used to discover CAN-2004-0786, and to SITIC for reporting the discovery of CAN-2004-0747.

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.0.51 is available for download from

<http://httpd.apache.org/download.cgi?update=200409150645>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see

http://httpd.apache.org/docs-2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following:

If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these modules to obtain this information.

[-- The Apache HTTP Server Project Team](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-09-15T19:26:03](#)

30 August 2004 - Apache HTTP Server Request Library 2.04-dev Released

Apache HTTP Server Request Library 2.04-dev Released The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the 2.04-dev release of libapreq2. This Announcement notes significant changes introduced by this release. The package libapreq2-2.04_03-dev.tar.gz is released under the Apache License version 2.0. It is now available through the ASF mirrors <http://httpd.apache.org/apreq/download.cgi> and has entered the CPAN as file: `$CPAN/authors/id/J/JO/JOESUF/libapreq2-2.04_03-dev.tar.gz` size: 592748 bytes md5: 1f5dd762c877b716f3774d502f575196 libapreq2 is an APR-based shared library used for parsing HTTP cookies, query-strings and POST data. The package libapreq2-2.04_03-dev.tar.gz provides 1) version 2.0.20 of the libapreq2 library, 2)

mod_apreq, a filter module necessary for using libapreq2 within the Apache HTTP Server, 3) the Apache::Request, Apache::Cookie, and Apache::Upload perl modules for using libapreq2 with modperl-2.

=====
Changes with libapreq2-2.04-dev (released August 30, 2004) - Perl API [joes] Add TAINT checks, marking all parsed data as tainted. - C API [joes] Add body_status attribute to apreq_request_t, to allow the both environment and the parser to report any errors encountered. - C API [randyk, joes] Cookie parser was locking up on non-alphanumeric chars in cookie names. Also RFC Cookie attributes are always checked for quotes during bake(2), and the quotes are now stripped from incoming RFC cookies during parsing (but they are never stripped from the actual cookie value). - Perl API [joes] Apache::Cookie::Jar->new accepts a VALUE_CLASS argument, which effectively blesses all the jar's cookies into that class, which simplifies subclassing Apache::Cookie. Accordingly Apache::Cookie->freeze(\$value) no longer accepts a freeze()-able object in \$value. - C API [Markus Wichitill, randyk, joes] Drop APR_DELONCLOSE from apreq_file_mktemp implementation and install apreq_file_cleanup. When passed to apr_file_open on Win32, APR_DELONCLOSE sets the FILE_SHARED_DELETE flag, which is, unfortunately, a property that is preserved across NTFS "hard" links. This breaks apps that link() the temp file to a permanent location, and subsequently expect...

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-08-30T23:22:49](#)

30 June 2004 - Apache HTTP Server 2.0.50 Released

Apache HTTP Server 2.0.50 Released

[The Apache Software Foundation](#) and [The Apache HTTP Server Project](#) are pleased to announce the release of version 2.0.50 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.50 as compared to 2.0.49. The Announcement is also available in German from:

<http://www.apache.org/dist/httpd/Announcement2.txt.de>

This version of Apache is principally a bug fix release. A summary of the bug fixes is given at the end of this document. Of particular note is that 2.0.50 addresses two security vulnerabilities:

A remotely triggered memory leak in http header parsing can allow a denial of service attack due to excessive memory consumption.

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0493>]

Fixes a mod_ssl buffer overflow in the FakeBasicAuth code for a (trusted) client certificate subject DN which exceeds 6K in length.

[\[http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0488\]](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0488)

This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade.

Apache HTTP Server 2.0.50 is available for download from

<http://httpd.apache.org/download.cgi>

Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes.

Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see

http://httpd.apache.org/docs-2.0/new_features_2_0.html

When upgrading or installing this version of Apache, please keep in mind the following:

If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these modules to obtain this information.

[- Apache HTTP Server Project Team](#)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-07-01T00:00:44](#)

11 May 2004 - Apache HTTP Server 1.3.31 Released

Apache HTTP Server 1.3.31 Released The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of version 1.3.31 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 1.3.31 as compared to 1.3.29 (1.3.30 was not released). The Announcement is also available in German, Spanish and Japanese from:

<http://www.apache.org/dist/httpd/Announcement.html.de>
<http://www.apache.org/dist/httpd/Announcement.html.es>
<http://www.apache.org/dist/httpd/Announcement.html.ja> (Original:
<http://www.apache.org/dist/httpd/Announcement.html>) This version of Apache is principally a bug and security fix release. A partial summary of the bug fixes is given at the end of this document. A full listing of changes can be found in the CHANGES file. Of particular note is that 1.3.31 addresses and fixes 4 potential security issues:

- o CAN-2003-0987 (cve.mitre.org) In mod_digest, verify whether the nonce returned in the client response is one we issued ourselves. This problem does not affect mod_auth_digest.
- o CAN-2003-0020 (cve.mitre.org) Escape arbitrary data before writing into the errorlog.
- o CAN-2004-0174 (cve.mitre.org) Fix starvation issue on listening sockets where a short-lived connection on a rarely-accessed listening socket will cause a child to hold the accept mutex and block out new connections until another connection arrives on that rarely-accessed listening socket. This only affects some platforms, such as Solaris, AIX and IRIX. Linux is unaffected.
- o CAN-2003-0993 (cve.mitre.org) Fix parsing of Allow/Deny rules using IP addresses without a netmask; issue is only known to affect big-endian 64-bit platforms

We consider Apache 1.3.31 to be the best version of Apache 1.3 available and we strongly recommend that users of older versions, especially of the 1.1.x and 1.2.x family, upgrade as soon as possible. No further releases will be made in the 1.2.x family. Apache 1.3.31 is available for download from:
<http://httpd.apache.org/download.cgi> This service utilizes the network of mirrors listed at: <http://www.apache.org/mirrors/> Please consult the CHANGES_1.3 file for a full list of...

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-05-11T09:07:44](#)

11 May 2004 - Press Release: Apache HTTP Server Technical Leadership

Press Release: Apache HTTP Server Technical Leadership Congratulations and kudos to the HTTP Server Project team for their hard work and accomplishments. To commemorate, the ASF issued this press release today: ----- Apache HTTP Server Reaches Record Eight Consecutive Years of Technical Leadership. San Francisco, CA (May 11, 2004) The Apache Software Foundation today announced that its HTTP Server platform has reached a milestone of eight consecutive years of World Wide Web technology leadership. Since its first release in April of 1995, the Apache HTTP Server has become as pervasive as the Web itself. According to two separate and independent surveys, the Apache HTTP Server, which originally established itself as the leading web server technology in April 1996, continues to acquire even

greater market, growing faster than all other competing web server technologies. We started the Apache project to provide the development community with a secure, efficient and extensible open source Web server platform. Our goal from the very beginning was to establish the Apache HTTP Server as the dialtone of the web a standards-compliant, commercial grade reference platform. Through collaboration with the community, we have continually improved upon and added modules to the core Apache HTTP Server platform, thereby evolving the quality and breadth of the technology, said Jim Jagielski, Executive Vice President and Secretary of the Apache Software Foundation. Our recent achievement is testament to the benefits of the process of open source software development itself. By collaborating with the community, we have been able to consistently deliver freely accessible, robust, feature-rich Web server technology. Apache HTTP Server Leadership Continues to Grow In an April 2004 Security Space survey of 14,174,836 Web sites, the Apache HTTP Server was recognized as the most widely implemented Web server platform, with 70.48% share, representing 9,990,804 deployed servers. In an April 2004...

Note:

Apache Software Foundation -- Posted by [Tetsuya Kitahata](#) at [2004-05-11T04:44:15](#)

19 March 2004 - Apache HTTP Server 2.0.49 Released

Apache HTTP Server 2.0.49 Released The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of version 2.0.49 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 2.0.49 as compared to 2.0.48. This version of Apache is principally a bug fix release. A summary of the bug fixes is given at the end of this document. Of particular note is that 2.0.49 addresses three security vulnerabilities: When using multiple listening sockets, a denial of service attack is possible on some platforms due to a race condition in the handling of short-lived connections. This issue is known to affect some versions of AIX, Solaris, and Tru64; it is known to not affect FreeBSD or Linux. [<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174>] Arbitrary client-supplied strings can be written to the error log which can allow exploits of certain terminal emulators.

[<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020>] A remotely triggered memory leak in mod_ssl can allow a denial of service attack due to excessive memory consumption.

[<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0113>] This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade. Apache HTTP Server 2.0.49 is available for download from

<http://httpd.apache.org/download.cgi> Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes. Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For an overview of new features introduced after 1.3 please see http://httpd.apache.org/docs-2.0/new_features_2_0.html When upgrading or installing this version of Apache, please keep in mind the following: If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these...

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-03-19T23:06:14](#)

03 March 2004 - Mod_python 3.1.3 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the 3.1.3 release of mod_python. Mod_python 3.1.3 is considered a stable release, suitable for production use. Mod_python is an Apache HTTP Server module that embeds the Python language interpreter within the server. With mod_python you can write web-based applications in Python that will run many times faster than traditional CGI and will have access to advanced features such as ability to maintain objects between requests, access to httpd internals, content filters and connection handlers. This release includes several features not available in the previous stable release (3.0.x). Some feature highlights: * Native cookie support, including support for automatic cryptographic cookie signing and marshalling. * Server-side sessions with memory or dbm-based storage and session locking support. * PSP - a fast flex-based scanner which allows embedding Python code within HTML. Mod_python 3.1.3 is released under the new Apache License version 2.0. Mod_python 3.1.3 is available for download from: <http://httpd.apache.org/modules/python-download.cgi> More information about mod_python is available at: [http://httpd.apache.org/modules/...](http://httpd.apache.org/modules/)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-03-03T19:15:57](#)

22 January 2004 - Mod_python 2.7.10 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of version 2.7.10 of mod_python. This release addresses a vulnerability in mod_python 2.7.9 whereby a specific query string

processed by mod_python would cause the httpd process to crash. The previously released version 2.7.9 was supposed to correct this issue, but is still vulnerable. There are no other changes or improvements from the previous version in this release. If you are currently using mod_python 2.7.9 or earlier, it is highly recommended that you upgrade to 2.7.10 as soon as possible. If you are using mod_python 3.0.4, no action is necessary. Mod_python is available for download from: <http://httpd.apache.org/modules/python-download.cgi> For more information about mod_python visit [http://www.modpython.org/...](http://www.modpython.org/)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2004-01-22T19:18:03](#)

28 November 2003 - Mod_python 3.0.4 and 2.7.9 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of versions 3.0.4 and 2.7.9 of mod_python. These two releases (for HTTP Server 2.0 and 1.3 respectively) address an issue whereby a specific query string processed by mod_python would cause the httpd process to crash. These two releases have also been patched to compile against Python 2.3 cleanly. There are no other changes or improvements from the previous version in these releases. Both of these releases are considered stable. If you are currently using mod_python 3.0.3 or 2.7.8, it is highly recommended that you upgrade to 3.0.4 or 2.7.9. Mod_python is available for download from: <http://httpd.apache.org/modules/python-download.cgi> For more information about mod_python visit [http://www.modpython.org/...](http://www.modpython.org/)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-11-28T19:21:33](#)

29 October 2003 - Apache HTTP Server 1.3.29 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of version 1.3.29 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 1.3.29 as compared to 1.3.28. The Announcement is also available in German from <http://www.apache.org/dist/httpd/Announcement.html.de>. This version of Apache is principally a bug and security fix release. A partial summary of the bug fixes is given at the end of this document. A full listing of changes can be found in the CHANGES file. Of particular note is that 1.3.29 addresses and fixes 1 potential security issue: o CAN-2003-0542 (cve.mitre.org) Fix buffer overflows in mod_alias and mod_rewrite

which occurred if one configured a regular expression with more than 9 captures. We consider Apache 1.3.29 to be the best version of Apache 1.3 available and we strongly recommend that users of older versions, especially of the 1.1.x and 1.2.x family, upgrade as soon as possible. No further releases will be made in the 1.2.x family. Apache 1.3.29 is available for download from:

<http://httpd.apache.org/download.cgi> This service utilizes the network of mirrors listed at: <http://www.apache.org/mirrors/> Please consult the CHANGES_1.3 file for a full list of changes. As of Apache 1.3.12 binary distributions contain all standard Apache modules as shared objects (if supported by the platform) and include full source code. Installation is easily done by executing the included install script. See the README.bindist and INSTALL.bindist files for a complete explanation. Please note that the binary distributions are only provided for your convenience and current distributions for specific platforms are not always available. Win32 binary distributions are based on the Microsoft Installer (.MSI) technology. While development continues to make this installation method more robust, questions should be directed to the news:comp.infosystems.www.servers.ms-windows newsgroup. For an overview of new features introduced after 1.2 please see...

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-10-29T04:19:06](#)

29 October 2003 - Apache HTTP Server 2.0.48 Released

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the eleventh public release of the Apache 2.0 HTTP Server. This Announcement notes the significant changes in 2.0.48 as compared to 2.0.47. This version of Apache is principally a bug fix release. A summary of the bug fixes is given at the end of this document. Of particular note is that 2.0.48 addresses two security vulnerabilities: mod_cgid mishandling of CGI redirect paths could result in CGI output going to the wrong client when a threaded MPM is used.

[<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0789>] A buffer overflow could occur in mod_alias and mod_rewrite when a regular expression with more than 9 captures is configured.

[<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0542>] This release is compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade. Apache 2.0.48 is available for download from <http://httpd.apache.org/download.cgi> Please see the CHANGES_2.0 file, linked from the above page, for a full list of changes. Apache 2.0 offers numerous enhancements, improvements, and performance boosts over the 1.3 codebase. For

an overview of new features introduced after 1.3 please see http://httpd.apache.org/docs-2.0/new_features_2_0.html When upgrading or installing this version of Apache, please keep in mind the following: If you intend to use Apache with one of the threaded MPMs, you must ensure that the modules (and the libraries they depend on) that you will be using are thread-safe. Please contact the vendors of these modules to obtain this information. For more information, see the Apache HTTP Server Project WebSite....

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-10-29T04:14:25](#)

27 October 2003 - Mod_python 3.1.2 Beta Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the 3.1.2 Beta release mod_python. Some feature highlights: * Server-side sessions with memory or dbm-based storage and session locking support. * PSP - a fast flex-based scanner which allows embedding Python code within HTML. * Native cookie support, including support for automatic cryptographic cookie signing and marshalling. * Compatibility with Python 2.3, as well as many other enhancements. Beta releases are NOT considered stable and may contain bugs. This release is intended to solicit widespread testing of the code. We strongly recommend that you try out your existing applications and experiment with new features in a non-production environment using this version and report any problems you may encounter so that they can be addressed before the final release. Preferred method of reporting problems is the mod_python user list mod_python@modpython.org. Mod_python 3.1.2b is available for download from: <http://httpd.apache.org/modules/python-download.cgi> For more information about mod_python visit [http://www.modpython.org/...](http://www.modpython.org/)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-10-27T19:22:55](#)

18 Jul 2003 - Apache HTTP Server 1.3.28 released

The Apache Software Foundation and The Apache Server Project are pleased to announce the release of version 1.3.28 of the Apache HTTP Server ("Apache"). This Announcement notes the significant changes in 1.3.28 as compared to 1.3.27. The Announcement is also available in German from <http://www.apache.org/dyn/closer.cgi/httpd/Announcement.txt.de>. This version of Apache is principally a bug and security fix release. A partial summary of the bug

fixes is given at the end of the release note document. A full listing of changes can be found in the CHANGES file. Of particular note is that 1.3.28 addresses and fixes 3 potential security issues: Apache HTTP Server 2.0.47 is available for download from <http://httpd.apache.org/download.cgi> - or - <http://www.apache.org/dyn/closer.cgi/httpd/> Apache is the most popular web server in the known universe; over half of the servers on the Internet are running Apache or one of its variants. IMPORTANT NOTE FOR APACHE USERS: Apache 1.3 was designed for Unix OS variants. While the ports to non-Unix platforms (such as Win32, Netware or OS2) are of an acceptable quality, Apache 1.3 is not optimized for these platforms. Security, stability, or performance issues on these non-Unix ports do not generally apply to the Unix version, due to software's Unix origin. Apache 2.0 has been structured for multiple operating systems from its inception, by introducing the Apache Portability Library and MPM modules. Users on non-Unix platforms are strongly encouraged to move up to Apache 2.0 for better performance, stability and security on their platforms. See The Apache HTTP Server Home Page for more details....

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-07-18T07:50:02](#)

09 Jul 2003 - Apache Http Server 2.0.47 released

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the tenth public release of the Apache 2.0 HTTP Server. This Announcement notes the significant changes in 2.0.47 as compared to 2.0.46. Apache Httpd WebServer 2.0.47 is available for download from <http://httpd.apache.org/download.cgi>. This version of Apache is principally a security and bug fix release. A summary of the bug fixes is given at the end of this document. Of particular note is that 2.0.47 addresses four security vulnerabilities. See The Apache HTTP Server Home Page for more details....

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-07-09T08:07:35](#)

28 May 2003 - Apache 2.0.46 released

The Apache Software Foundation and the Apache HTTP Server Project are pleased to announce the ninth public release of the Apache 2.0 HTTP Server. This Announcement notes the significant changes in 2.0.46 as compared to 2.0.45. This version of Apache is principally a security and bug fix release. This release is

compatible with modules compiled for 2.0.42 and later versions. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade. See The Apache HTTP Server Home Page for more details....

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-05-28T08:20:30](#)

02 April 2003 - Apache 2.0.45 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the eighth public release of the Apache 2.0 HTTP Server. This version of Apache is principally a security and bug fix release. A summary of the bug fixes is given at the end of this document. Of particular note is that 2.0.45 addresses two security vulnerabilities, both affecting all platforms. We consider this release to be the best version of Apache available and encourage users of all prior versions to upgrade. Apache 2.0.45 source code is available for download from here. Apache 2.0.45 binary releases will become available for download from here Please remember to check the signature when downloading from a mirror....

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-04-02T08:46:44](#)

17 March 2003 - Mod_python 3.0.3 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of mod_python 3.0.3. Mod_python is an Apache HTTP Server module that embeds the Python interpreter within the server. With mod_python you can write web-based applications in Python that will run many times faster than traditional CGI and will have access to advanced features such as ability to retain database connections between requests, access to httpd internals and provide content filter as well as connection handlers. This release fixes numerous bugs identified after last release (3.0.1). It is highly recommended that you upgrade to version 3.0.3 for improved stability and performance. Mod_python is available for download from: <http://httpd.apache.org/modules/python-download.cgi> For more information about mod_python visit: [http://www.modpython.org/...](http://www.modpython.org/)

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2003-03-17T21:28:05](#)

28 November 2002 - Mod_python 3.0.1 Released

The Apache Software Foundation and The Apache HTTP Server Project are pleased to announce the release of mod_python 3.0.1. Mod_python is an Apache HTTP Server module that embeds the Python interpreter within the server. With mod_python you can write web-based applications in Python that will run many times faster than traditional CGI and will have access to advanced features such as ability to retain database connections between requests, access to httpd internals and provide content filter as well as connection handlers. This is the first release of mod_python as a subproject of the Apache HTTP Server Project, as well as a major milestone accomplishment finally bringing compatibility with Apache 2.0. This release increments the major version to 3. The major version increment is to denote that this release is only compatible with Apache httpd server 2.0 and Python 2.2 or later and is not fully backwards compatible with previous versions of mod_python. For details on migrating code from previous versions of mod_python, as well as a list of new features, see the README file in the distribution. Mod_python is available for download from: <http://www.apache.org/dist/httpd/modpython/> For more information about mod_python visit <http://www.modpython.org/> Enjoy, and Happy Thanksgiving to those in the US!...

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2002-11-28T21:26:27](#)

13 September 2002 - Mod_Python donated to ASF

It is my pleasure to announce that Mod_Python has been donated to the Apache Software Foundation, and is now a subproject of the httpd server project (see <http://httpd.apache.org/>). I am grateful to ASF for accepting this donation and committing resources to further the support of Mod_Python. I believe that this action will advance the development of Mod_Python, resulting in an ultimately better and more popular tool for Python developers. I also believe it will serve to better position Python as a language of choice for web development, a need that has been expressed by many. There are no implications to the current Mod_Python users - the license is the same with the sole difference in that the copyright belongs to ASF now. As a consequence of the donation, the CVS repository is now hosted on cvs.apache.org. Do not use the SourceForge repository anymore, it will soon be removed. There will also be website and mailing changes, but the details are still being finalized and will be announced when ready....

Note:

Apache HTTP -- Posted by [Tetsuya Kitahata](#) at [2002-09-13T21:21:18](#)