

Apache 1.3.27 Launched! - Developer News

NEWS_PDF_AUTHOR: w4z004

NEWS_PDF_DATE: 2002/10/4 14:07:06

There is a new Apache released and this time its version 1.3.27. **Security vulnerabilities** The main security vulnerabilities addressed in 1.3.27 are:

- Fix the security vulnerability noted in CAN-2002-0839 (cve.mitre.org) regarding ownership permissions of System V shared memory based scoreboards. The fix resulted in the new ShmemUIDisUser directive.
- Fix the security vulnerability noted in CAN-2002-0840 (cve.mitre.org) regarding a cross-site scripting vulnerability in the default error page when using wildcard DNS.
- Fix the security vulnerability noted in CAN-2002-0843 (cve.mitre.org) regarding some possible overflows in ab.c which could be exploited by a malicious server.

New features

The main new features in 1.3.27 (compared to 1.3.26) are:

- The new ErrorHandler directive has been added.
- Configuration file globbing can now use simple pattern matching.
- The protocol version (eg: HTTP/1.1) in the request line parsing is now case insensitive.
- ap_snprintf() can now distinguish between an output which was truncated, and an output which exactly filled the buffer.
- Add ProtocolReqCheck directive, which determines if Apache will check for a valid protocol string in the request (eg: HTTP/1.1) and return HTTP_BAD_REQUEST if not valid.
- Versions of Apache prior to 1.3.26 would silently ignore bad protocol strings, but 1.3.26 included a more strict check. This makes it runtime configurable.
- Added support for Berkeley-DB/4.x to mod_auth_db.
- httpd -V will now also print out the compile time defined HARD_SERVER_LIMIT value.

New features that relate to specific platforms:

- Support Caldera OpenUNIX 8.
- Use SysV semaphores by default on OpenBSD.
- Implemented file locking in mod_rewrite for the NetWare CLib platform.

Bugs fixed The following bugs were found in Apache 1.3.26 and have been fixed in Apache 1.3.27:

mod_proxy fixes:

- The cache in mod_proxy was incorrectly updating the Content-Length value from 304 responses when doing validation.
- Fix a problem in proxy where headers from other modules were added to the response headers when this was already done in the core already.
- In 1.3.26, a null or all blank Content-Length field would be triggered as an error; previous versions would silently ignore this and assume 0. 1.3.27 restores this previous behavior.
- Win32: Fix one byte buffer overflow in ap_get_win32_interpreter when a CGI script's #! line does not contain a or (i.e. a line feed character) in the first 1023 bytes. The overflow is always a " (string termination) character.

[Download Apache 1.3.27](#)

There is a new Apache released and this time its version 1.3.27. **Security vulnerabilities** The main security vulnerabilities addressed in 1.3.27 are:

- Fix the security vulnerability noted in CAN-2002-0839 (cve.mitre.org) regarding ownership permissions of System V shared memory based scoreboards. The fix resulted in the new ShmemUIDisUser directive.
- Fix the security vulnerability noted in CAN-2002-0840 (cve.mitre.org) regarding a cross-site scripting vulnerability in the default error page when using wildcard DNS.
- Fix the security vulnerability noted in CAN-2002-0843 (cve.mitre.org) regarding some possible overflows in ab.c which could be exploited by a malicious server.

New features

The main new features in 1.3.27 (compared to 1.3.26) are:

- The new ErrorHandler directive has been added.
- Configuration file globbing can now use simple pattern matching.
- The protocol version (eg: HTTP/1.1) in the request line parsing is now case insensitive.
- ap_snprintf() can now distinguish between an output which was truncated, and an output which exactly filled the buffer.
- Add ProtocolReqCheck directive, which determines if Apache will check for a valid protocol string in the request (eg: HTTP/1.1) and return HTTP_BAD_REQUEST if not valid.
- Versions of Apache prior to 1.3.26 would silently ignore bad protocol strings, but 1.3.26 included a more strict check. This makes it runtime configurable.
- Added support for Berkeley-DB/4.x to mod_auth_db.
- httpd -V will now also print out the compile time defined HARD_SERVER_LIMIT value.

New features that relate to specific platforms:

- Support Caldera OpenUNIX 8.
- Use SysV semaphores by default on OpenBSD.
- Implemented file locking in mod_rewrite for the NetWare CLib platform.

Bugs fixed The following bugs were found in Apache 1.3.26 and have been fixed in Apache 1.3.27:

mod_proxy fixes:

- The cache in mod_proxy was incorrectly updating the Content-Length value from 304 responses when doing validation.
- Fix a problem in proxy where headers from other modules were added to the response headers when this was already done in the core already.
- In 1.3.26, a null or all blank Content-Length field would be triggered as an error; previous versions would silently ignore this and assume 0. 1.3.27 restores this previous behavior.
- Win32: Fix one byte buffer overflow in ap_get_win32_interpreter when a CGI script's #! line does not contain a or (i.e. a line feed character) in the first 1023 bytes. The overflow is always a " (string termination) character.

[Download Apache 1.3.27](#)