

[UNIX] Remote Heap Corruption Overflow vulnerability in WsMp3d (CHA)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0041.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/21/03

To: list@securiteam.com

Date: 21 May 2003 18:59:31 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Remote Heap Corruption Overflow vulnerability in WsMp3d (CHA)

SUMMARY

<<http://wsmp3.sourceforge.net>> WsMp3d is a "web server which also acts as a ShoutCast-server". A remotely exploitable heap vulnerability allows attackers to cause the program to execute arbitrary code.

DETAILS

Due to misallocation and incorrect utilization of resources, a heap overflow vulnerability can be caused by a remote attacker, allowing him to execute arbitrary code.

Patch:

--- req_descriptor.c Mon Dec 2 22:21:35 2002

+++ req_descriptor.patch.c Sat May 3 03:25:32 2003

@@ -201,11 +201,11 @@

```
    if(PDEBUG) printf("Entro in parse_request\n");
```

```
    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
```

Securiteam: [UNIX] Remote Heap Corruption Overflow vulnerability in WsMp3d (CHA)

```
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(10-1));
  ritorno->action=get_op(reqcpy);

  for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
  if(ritorno->action!=NULL)
  {
    if(!strcmp(ritorno->action,"CHA"))
ritorno->what=nomefile(reqcpy,1) ;
@@ -214,55 +214,55 @@
    else ritorno->what=NULL;

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->host=gimme_line(reqcpy,"Host: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->agent=gimme_line(reqcpy,"User-Agent: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->accept=gimme_line(reqcpy,"Accept: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->lang=gimme_line(reqcpy,"Accept-Language: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->enc=gimme_line(reqcpy,"Accept-Encoding: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->charset=gimme_line(reqcpy,"Accept-Charset: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
    ritorno->keep=gimme_line(reqcpy,"Keep-Alive: ");

    for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
```

Securiteam: [UNIX] Remote Heap Corruption Overflow vulnerability in WsMp3d (CHA)

```
+ strncpy(reqcpy,req,(1024-1));
ritorno->conn=gimme_line(reqcpy,"Connection: ");

for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
ritorno->referer=gimme_line(reqcpy,"Referer: ");

for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
ritorno->pragma=gimme_line(reqcpy,"Pragma: ");

for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
ritorno->contentType=gimme_line(reqcpy,"Content-Type: ");

for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
ritorno->contLength=gimme_line(reqcpy,"Content-Length: ");

for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
- strncpy(reqcpy,req,strlen(req));
+ strncpy(reqcpy,req,(1024-1));
ritorno->content=gimme_content(reqcpy);
for(i=0;i<BUFSIZE;i++) reqcpy[i]='\0';
return ritorno;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:xploit@hackermail.com>>
dong-h0un U.

=====

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.