

ListLib

19Feb2004

ListLib is a ShareWare product from GreenHouse. It prevents a Denial of Service (DoS) attack through the FTP port: A possible attacker can use his FTP client to start as many FTPSERV processes on the Tandem system, until the number of processes, or swap space, or other resources, are exhausted and no further service from the system is granted.

Function

The tool is designed as a library, which becomes part of the LISTNER product on the Tandem system. It intercepts the Process_Create_ procedure call and, before the call is executed, it checks the number of already running FTPSERV processes. In case the found number of processes exceeds the number of configured ones, or in case the number of still logged off FTPSERV processes exceeds a configured number, no new FTPSERV process is created.

The library does not react proactive in case a DoS happens, but it prevents the NSK system from running into trouble by that type of attack.

LISTCONF

To make the library as flexible as possible, the following attributes can be configured through an EDIT type file named LISTCONF. This file has to reside in the same location in which LISTLIB resides.

The following key words are supported:

EMSCollector

All LISTLIB actions are reported to the EMS system. In case the EMS collector is not \$0, its name has to be configured here.

In case the entry is missing, \$0 is assumed as the default collector process.

Default is: \$0

MAXNUMPROCS

Before Listner denies the creation of a new process, a defined number of processes already has to exist. The number can be any value between 1 and 1000. In case the number is out of range, it is assumed to be 5.

Default is: 5

MAXNUMLOGGEDOFF

Before Listner denies the creation of a new process, a defined number of still logged off processes might exist. The number can be any value between 1 and 1000. In case the number is out of range, it is assumed to be 5.

Default is: 5

PROGRAMFILE

The Listner library needs to know program file names to find the number of already running processes, derived from a given object. To make this as flexible as possible, you can define the program file names as templates.

All wildcard characters are supported.

Entries are NOT case sensitive.

The number of program file templates is limited to 100.

*Default is: *. *FTPSERV**

This LISTCONF EDIT type file has to reside in the same location as the LISTLIB file.

Changes in the library are automatically taken into account: Restarting the LISTNER process is NOT required.

Installation

To add this library to the LISTNER process, perform these steps:

1. EDIT the LISTCONF configuration file and adjust it to your needs.
2. Stop the LISTNER process in question. This does NOT interrupt already running FTP sessions. While the LISTNER is stopped, no new LISTNER controlled sessions can be started.
3. Use the BINDLIB¹ tool to bind the LISTLIB product to the LISTNER:
`BINDLIB [/OUT <file>/] $SYSTEM.SYSnn.LISTNER WITH $vol.subvol.LISTLIB`
4. Re-start the LISTNER process

De-Installation

1. Stop the LISTNER process in question. This does NOT interrupt already running FTP sessions. While the LISTNER is stopped, no new FTP sessions can be started.
2. Use the BINDLIB tool to un-bind the LISTLIB product to the LISTNER:
`BINDLIB [/OUT <file>/] $SYSTEM.SYSnn.LISTNER`
3. Re-start the LISTNER process

¹ BINDLIB is a freeware tool from Greenhouse. It can be found at www.GreenHouse.de

LISTFTP

LISTLIB keeps track of the FTPSERV processes by using a disk file, named LISTDAT. This file is located in the same location as the LISTLIB object file.

LISTFTP can be used to display all active FTPSERV sessions along with some session attributes:

```
$GHS1 LISTNER 128> listftp
  IP Address          Start Time          Object File Name      Logged On
-----
192.231.036.081  19 Feb 2004, 13:36  $GHS1.FTP.FTPSERVT    No
$GHS1 LISTNER 129>
```

LISTFTP has to reside in the same location in which LISTLIB resides.

