Technical Information Bulletin

TIBID# DSI140930
Date: 1/30/2015
Importance: High

Title: GHOST Vulnerability for various DSI VTL models

Description of Problem: Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST." As you are aware the DSI VTL product runs on various Linux distributions. A patch has been published which resolves the vulnerability in our DSI 300-, 350-, and older 9000- series VTL products.

Verify Vulnerability: Any version of glibc before **version 2.5-123** is vulnerable. To determine what version is installed on your system, log in using Putty & run following command.

- # rpm –qa | grep glibc

Solution: Apply **glibc updates** using the enclosed instructions.

Any questions about this TIB should be directed to DSI support at the following email address.

SUPPORT@DYNAMICSOLUTIONS.COM

Thank you;
DSI
Customer Support
(800) 641-5215

Prerequisites

Please confirm the appropriate tools have been installed on your Windows PC.

1. PuTTy download site:
   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

2. WinSCP download site:
   http://winscp.net/eng/download.php

Determine your operating system:

Log into your VTL system using putty & run the following command to determine your operating system.

 # vtl version then run **# uname -a** and match it below:

DSI VTL Server Version	Kernel Version	OS Version	Hardware Platforms
v2.0	2.6.9-22.el5	CentOS v5.0	DSI9000 Series
v2.1	2.6.18-53.1.19.el5	CentOS v5.1	DSI9000 Series
v2.2	2.6.18-194.11.4.el5	CentOS v5.5	DSI9000 Series
v3.0	2.6.18-194.11.4.el5	Oracle Enterprise Linux (OEL) v5.5	DSI300 Series Only
v3.5	2.6.18-274.el5	Oracle Enterprise Linux (OEL) v5.7	DSI350 Series Only

Downloads

Please download the 3 appropriate patches based on your operating system to the downloads folder on your Windows PC prior to completing the patch installation.

a. **Oracle Linux:**

http://public-yum.oracle.com/repo/OracleLinux/OL5/latest/x86_64/getPackage/glibc-2.5-123.0.1.el5_11.1.x86_64.rpm
http://public-yum.oracle.com/repo/OracleLinux/OL5/latest/x86_64/getPackage/glibc-2.5-123.0.1.el5_11.1.i686.rpm
http://public-yum.oracle.com/repo/OracleLinux/OL5/latest/x86_64/getPackage/glibc-common-2.5-123.0.1.el5_11.1.x86_64.rpm

b. **CentOS**:

http://mirror.centos.org/centos/5/updates/x86_64/RPMS/glibc-2.5-123.el5_11.1.i686.rpm
http://mirror.centos.org/centos/5/updates/x86_64/RPMS/glibc-2.5-123.el5_11.1.x86_64.rpm
http://mirror.centos.org/centos/5/updates/x86_64/RPMS/glibc-common-2.5-123.el5_11.1.x86_64.rpm

** This patch requires a reboot **

Installation

Schedule a maintenance window for this patch to ensure you can reboot the system as required. Complete the following steps to patch your VTL system. Please contact DSI support if you require additional assistance.

Download the following rpm packages from the links above:

glibc-2.5-123.el5_11.1.i686.rpm
glibc-2.5-123.el5_11.1.x86_64.rpm
glibc-common-2.5-123.el5_11.1.x86_64.rpm

1. Suspend failover from the VTL console (if applicable)
   - # **Right click on the server > Select failover > Select stop takeover**
2. Login to your VTL server using the WinSCP utility.
3. Transfer the downloaded files to the /root/ directory of the VTL.
4. Login to your VTL server using the PuTTy utility, navigate to the /root/ directory.
   - # **cd /root**
5. Run the following command to install the patches:
   - # **rpm -Uvh --repackage glibc-2.5-123.el5_11.1.i686.rpm glibc-2.5-123.el5_11.1.x86_64.rpm glibc-common-2.5-123.el5_11.1.x86_64.rpm**
6. Reboot the server from the VTL console
   - # **Right click the server > Select system maintenance > Select Reboot**
7. Update is now complete.
8. Enable failover from the VTL console once both systems are patched (if applicable)
   - # **Right click on the server > Select failover > Select start takeover**

==========

Contact Info:

All questions or concerns regarding this document should be directed to support@dynamicsolutions.com or (800) 641-5215.