Operations Alert Bulletin Recommended Patch for All DBDS Platforms Using Solaris 10

Background

Cisco engineers have discovered that Solaris 10 has a security vulnerability in the telnet daemon **in.telnetd**. This security vulnerability allows users to obtain root access to Cisco's Digital Broadband Delivery System (DBDS) platform through telnet—without the need for the root password. *If this vulnerability is not corrected, users can access root or any other user ID without a password.*

All DBDS system operators running System Release (SR) versions 2.7/3.7 or SR 4.2 are affected by this vulnerability.

The engineering team has developed software patch **4.2.0.5p1** to remedy this security issue. Change request (CR) **67457** addresses this security issue.

Cisco has made this security patch available, through a compressed file, on the Cisco FTP server. Because this patch can be installed without a need for a system reboot, Cisco urges system operators to install this patch immediately.

For additional background information, see Sun Microsystems' Support Web page (reference **Sun Alert 102802-1**).

Requirement

All system operators running Solaris 10 must install software patch **4.2.0.5p1**. This impacts systems running SR 2.7/3.7 and SR 4.2.

Recommendation

Cisco urges all system operators running SR 2.7/3.7 or SR 4.2 to obtain and install patch **4.2.0.5p1** immediately on their DNCS, Application Server, and RNCS, if the site is equipped with an RNCS.

Important! This patch can be installed without the need for a system reboot.

About This Bulletin

Audience

This document is intended for system operators of Cisco's DBDS who run SR 2.7/3.7 or SR 4.2 software. No other system releases are affected.

Document Version

This is the first release of this document.

Obtain and Install the Security Software Patch

The procedures in this section provide general instructions to obtain, extract, and install the Security Software Patch.

Obtaining the Security Software Patch

The following procedure provides generic steps to directly download software from the FTP server onto the DNCS. Because many sites do not allow an open Internet connection to the DNCS for security reasons, this procedure provides generic instructions to access the FTP server and download the software onto the DNCS.

Follow these general instructions to obtain the compressed file that contains the Security Software Patch.

1. On the DNCS, create a directory called **download** in the /export/home/dncs directory structure (mkdir /export/home/dncs/download).
2. Log on to the Cisco FTP server.

   Notes:

   - The address of the server is **ftp.sciatl.com** or **192.133.243.133**.

     Note: The address for the Cisco FTP server is subject to change. If you are unable to reach the FTP server, please contact Cisco Services for the latest address.
   - The username is **anonymous**.
   - The password is the email address of the person logging in.
3. Choose one of the following options to navigate to the directory in which the file is located:
   - If you are *outside* of Cisco's firewall, type **cd /pub/scicare/RELEASED/SR4.2EmergencyPatches**
   - If you are *inside* of Cisco's firewall, type **cd /external_pub/scicare/RELEASED/SR4.2EmergencyPatches**
4. Type **bin** and press **Enter**. The system sets the ftp transfer mode to binary.
5. Type **hash** and press **Enter**. The system configures itself to display hash marks that show file-transfer progress.
6. Type **prompt** and press **Enter**. The system indicates that interactive mode is off.
7. Type **get 4.2.0.5p1_SolarisPatch.tar.gz** and then press **Enter**. The system begins copying the file from the FTP server to the current directory on the DNCS.
8. Type **bye** and press **Enter** to log out of the Cisco FTP server.

Extracting the Security Software Patch

After obtaining the compressed file from Cisco's FTP site, follow these instructions to uncompress and extract the patch.

1 From an xterm window on the DNCS, type **cd /export/home/dncs/download** and then press **Enter**.

2 Type **gzip -d 4.2.0.5p1_SolarisPatch.tar.gz** and then press **Enter**. The system uncompresses the file that has just been downloaded.

3 Type **tar xvf 4.2.0.5p1_SolarisPatch.tar** and then press **Enter**. The system creates a subdirectory that contains a readme file (with installation instructions), as well as executable and supporting files.

Installing the Security Software Patch

Use the text editor of your choice to open the readme file. Carefully review and follow the patch installation instructions provided in the readme file.

Note: If you have any questions or concerns, contact Cisco Services before you begin the installation process.

Remember Cisco's recommendation:

- All sites running SR 2.7/3.7 and SR 4.2 must install 4.2.0.5p1 immediately on their DNCS, Application Server, and RNCS, if the site is equipped with a RNCS(s).
- You can install this patch file at any time without the need for a system reboot.

For More Information

If you have additional technical questions, call Cisco Services. Follow the menu options to speak with a service engineer.

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

Product and service availability are subject to change without notice.

April 2012 Printed in USA Part Number 4015090 Rev B