dynamic
solutions
international

Technical Information Bulletin

TIBID# DSI140929
Date: 09/29/2014
Importance: High

Title: BASH Shell Shock Vulnerability for DSI 3xx VTL models

Description of Problem: A remotely exploitable vulnerability has recently been discovered that affected most Linux distributions (CVE-2014-6271, CVE-2014-7169). As you are aware the DSI VTL product runs on various Linux distributions. We have created a patch that resolves the bash module vulnerability in our DSI 300-, 350-, and older 9000- series VTL products.

Solution: Apply VTL patch **update-rhel5x04** 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 insure that the following has been downloaded on your Windows PC prior to completing the patch installation.

1. Direct DSI VTL bash patch download:
   http://support.dynamicsolutions.com/FileDownload.aspx?ID=43214

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

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

Installation

Please complete the following steps to patch your VTL system. Please contact DSI support if you require additional assistance.

1. Login to your VTL server using the WinSCP utility.

2. Upload the file 'update-rhel5x04' to the /root/ directory of the VTL.

3. Login to your VTL server using the PuTTy utility, navigate to the /root/ directory.

   ```
   #cd /root
   ```

4. Run the following command to make the patch file executable:

   ```
   #chmod  +x  update-rhel5x04
   ```

5. Run the following command to apply the patch:

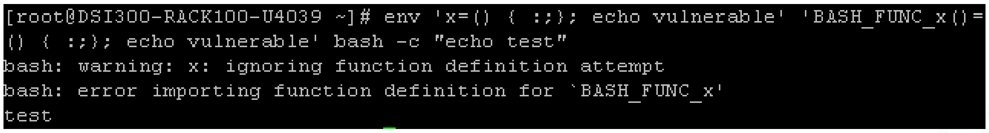
   ```
   #./update-rhel5x04
   ```

6. Update is now complete.

Verification

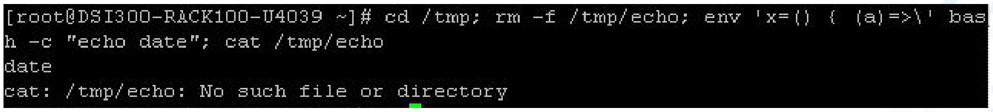
7. To verify patch success run the following commands via the PuTTy. The commands may be cut and pasted into the PuTTy window. The output of the scripts should be exactly as indicated below. If there is any variance please contact DSI support for additional assistance.

- # **env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=() { :;}; echo vulnerable' bash -c "echo test"**



```
[root@DSI300-RACK100-U4039 ~]# env 'x=() { :;}; echo vulnerable' 'BASH_FUNC_x()=
() { :;}; echo vulnerable' bash -c "echo test"
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `BASH_FUNC_x'
test
```

- # **cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>\' bash -c "echo date"; cat /tmp/echo**

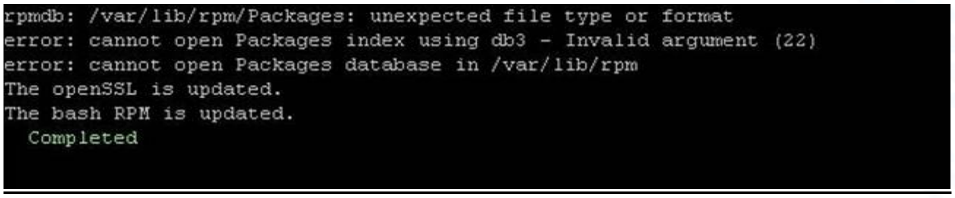


```
[root@DSI300-RACK100-U4039 ~]# cd /tmp; rm -f /tmp/echo; env 'x=() { (a)=>\' bas
h -c "echo date"; cat /tmp/echo
date
cat: /tmp/echo: No such file or directory
```

==

Note:

In the unlikely event the rpm database is corrupt with the following error message(s)



```
rpmdb: /var/lib/rpm/Packages: unexpected file type or format
error: cannot open Packages index using db3 - Invalid argument (22)
error: cannot open Packages database in /var/lib/rpm
The openSSL is updated.
The bash RPM is updated.
  Completed
```

You need to run the following commands to rebuild the rpm database needed to install the patch

# **cd /var/lib**
# **mkdir rpm-backup**
# **cp –a __db.* /var/lib/rpm-backup**
# **cd /var/lib/rpm-backup**
ls
# **rpmdb –rebuilddb**

And attempt to install the patch again.

Contact Info:

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