Shellshock Bash Vulnerability

What is it?

A critical vulnerability has been reported in the GNU Bourne-Again Shell (also known as Bash), the common command-line shell used in many Linux/UNIX operating systems and Apple's Mac OS X. This flaw could allow an attacker to remotely execute shell commands by attaching malicious code in environment variables used by the operating system.

Are Exacq products affected?

Exacq does not believe that any current exacqVision software packages have direct vulnerability associated with Bash. However, several Ubuntu/Linux core operating system components and other software used within the operating system are affected. Also, exacqVision Web Service versions released before December 2013 are vulnerable (versions 3.2.1 and later are not affected).

How do I protect my systems?

NOTE: As the Linux community improves its solutions to patch the vulnerable code, this article will be updated with new information. Please revisit this article periodically to check for any changes. (Permalink: https://exacq.com/kb/?crc=13518)

Currently, there are several things you can do to limit the situations that could make your system vulnerable:

1. Make sure exacqVision Web Service is updated (https://exacq.com/support/downloads.php).

2. Use static IP addresses to reduce vulnerability, as DHCP is affected.

3. Update Bash to the latest version using one of the following options:

   a) Browse to https://exacq.com/files and click the Shellshock folder. Download the .deb file and copy it to the Ubuntu Desktop. Double-click the file and wait for the patch to install.

   b) Open a command prompt and run the following commands:

```
sudo apt-get update
sudo apt-get install bash
```

NOTE: **All exacqVision systems shipped after October 6, 2014 will have the latest Bash version installed at the time of manufacture.**

For more information, please read this article from Ubuntu.

NOTE: If you are running 8.04 Ubuntu, these patches will not work. You must either upgrade your server to 10.04 Ubuntu or higher, or apply a third-party patch. Exacq has tested the patch at the following location and has not found any issues with the DEB file near the bottom of the page: http://uwekamper.de/how-i-patched-the-gnu-bash-shellshock-bug-on-ubuntu-804-hardy-heron.html