QI Partners Security Alert

9/25/2014

Eric Hummel, Founder and CTO, QI Partners

Bash Vulnerability - aka Shellshock (CVE-2014-6271)

A major software vulnerability was announced today that affects Linux, Unix and Mac OSX systems. It does not affect most Windows systems unless they are running the affected Operating Systems as virtual machines. Nearly all Linux and Mac OSX system are affected. Because of the seriousness of the vulnerability all systems should be checked.
The vulnerability is a bug that affects a very core component of the Operating System called the "Shell". “Bash" is the most common shell in the Unix/linux world. It is a general purpose tool used by all system administrators to load, maintain, run and delete software and files. It has enormous control, and in the wrong hands potential for misuse. The most likely path for exploitation is through a web server. Systems running a web service can easily be compromised with this bug. Apache, nginx and many other web servers will allow a malicious script to exploit this bug.

Special concern for Health IT: Many systems that are not core servers run legacy Operating Systems including Linux. These systems are rarely patched or serviced and tend to run for many years without any maintenance. Although it was recently announced, it is present in systems that are as much as 20 years old. Many of these system use web servers (e.g. apache) to connect with consoles, external computers or servers.

Recommendations:

1. Your IT Staff should be aware of this vulnerability. However, it is serious enough that you should not take this for granted. Call them and get from them the remediation plan for removing the bug. **Do not delay**. Cleaning up a compromised system is not something you want to do.
2. Start with externally accessible devices, especially internet facing Servers. Also check the network devices such as firewalls and wireless routers which sometimes run Linux. Continue until all devices are patched.
3. Remediation is not very difficult and may take only a few minutes per device if the technician is skilled, but does require access and knowledge of the shell. Nearly all of the vendors have issued patches. Many of these patches can be installed without an interruption in service.
4. Take this opportunity to review the Operating System version on each device in your network. This should be recorded in your IT inventory. This way you can immediately respond to the most vulnerable and critical devices first.
5. Spread the word. This vulnerability has the potential of being a serious problem if left unpatched.

© QI Partners, LLC 2014