**Briefing Note**

**Issue**

Early Wednesday morning, Information Security Services (ISS) was made aware of a key vulnerability in Linux and MAC OS X platforms that has been named “Shellshock/Bash”. Any device based on Linux/OS X could be susceptible. While it is still unknown how exploitable this bug is, if an attacker can exploit this bug, then they could gain access to internal data, reconfigure environments and insert malicious code.

**Background**

Every computer operating system has what's called a command shell, which is a means for a user to interface with the computer's operating system through direct commands.  These days, most users interface with the system using a graphical user interface.  IT staff and programmers are usually the ones who use the command shell.  In the Unix/Linux world, there are different shells available.  Over the last ten years, the "Bash" shell has gained enormous popularity given it is favoured by the Linux and open source systems movement.  When Apple moved their platform to a Unix base, they adopted the Bash shell as well.

Command shells, such as Bash, provide a means for systems managers to write small programs, called scripts that can execute interactively, or automatically.  In the Linux/Unix world, the functioning of the system is very much dependent on a collection of scripts that call other scripts, which call more scripts, and so on.  Compared to a proper programming language, the functionality of the command shell is limited - however, Bash is one of the more featured shells.

All computer programs and scripts need to be initialized in some way, such as an instruction on where on the disk to find other scripts/programs.  This collection of initializations is called the "environment", which can be modified during the execution of the program or script.

A security researcher in Europe recently figured out that one can define a script subroutine (containing a command) in the environment such that it will execute when Bash is run.

What this means is that if an environment containing this command is given to a webserver, for example, while the web server software itself may ignore that environment, it may need to run a script, using that Bash shell that will execute the command.  The command provided could be malicious, since it's passed over the public Internet.  While any non-Windows device is vulnerable because it's probably running Bash, the means to exploit the vulnerability is quite variable since it depends on an Internet service accepting that "malicious" environment, and executing a script.

**Nature of the Threat**

The first class of risk is against mass-produced/commodity platforms, like portable disk appliances (often just embedded Linux devices few vendors patch) widely used by faculty members or perhaps poorly-secured small applications, calendars, etc. Incursions can most likely be detected as a nuisance scan and issues can be addressed as they arise.

The other class could be highly specific and targeted. These are likely to take longer for attackers to sort out in terms of specific attacks. This will buy time for patches to be developed and implemented to lower the risk.

**What’s Being Done**

Ongoing monitoring and scanning is being done by the ISS team. The current focus is to look at Unix/Linux-based web servers that run other scripts since these are the most likely to be exploitable.

The investment made in the Campus firewall will help with unintended exposures (like inappropriately configured disk arrays and SCADA equipment). The corporate environment is fully behind the firewall. By December, the far majority of faculties will have their key servers behind the firewall.

IST has been applying patches immediately as they become available. IST is also working closely with the faculties to identify and patch platforms at risk.

The overall IT industry and open source community response has been a lot of noise so far, with few specific signals on solving the issue. That should settle down over the next few days and IST and the Faculty IT staff will work together to implement any resulting solutions to address the long term risks noted on the previous page.

Information Systems Technology

September 25, 2014