

Entuity Software Notification

Technical Bulletin

Version 2014.09.26

September 26, 2014

Bash "ShellShock" Vulnerability

A major security vulnerability has been discovered on Unix and Linux servers that run the command shell "**Bash**". The vulnerability has been named "**Shellshock**". The purpose of this notification is to explain why Entuity software **does not expose** users to this vulnerability and to provide references to further information on the subject.

The vulnerability allows code to be injected into and executed by Bash shell scripts via parsing of environment variables. Web servers configured to use the Common Gateway Interface (CGI) are at particular risk since environment variables are employed to pass URL arguments to the executed CGI programs or scripts. This means that malicious code can be entered as a web browser URL on a local workstation, which is then injected into and run by a CGI Bash shell script on a remote web server.

It is important to note that this particular vulnerability is only exposed when a web server is configured to run CGI Bash shell scripts. Entuity software does incorporate a CGI enabled web server; however, all of the CGIs supplied by Entuity are compiled binary files. There are no CGI Bash scripts distributed with the Entuity software product, and as a consequence **Entuity does not expose the Shellshock vulnerability**.

The manufacturers of the software products affected by Shellshock have already issued patches. We recommend you refer to the following web-sites for further information on the subject.

RedHat Linux:

<https://access.redhat.com/articles/1200223>

GNU Bash:

<http://www.fsf.org/news/free-software-foundation-statement-on-the-gnu-bash-shellshock-vulnerability>