Product Bulletin

Industrial Networking

Topic: Shellshock Bash Vulnerability **Date:** October 2014

Red Lion Controls has conducted a review of our products relative to the recently reported "Shellshock" bash vulnerabilities as documented in US-CERT CVE-2014-6271 and CVE-2014-7169. None of our products, which include Red Lion, Sixnet and N-Tron brands, are impacted by the bash vulnerabilities.

The majority of our products do not use the affected bash shell and should be considered immune to this issue. The following products do utilize the bash shell, but are not vulnerable. However, action may be required:

Sixnet BT-5000 and 6000 Series

The affected bash shell is running as part of the system process, deep in the runtime environment. No direct user access is available to reach the bash shell and execute the vulnerability. Bash will be updated with the latest security patches to resolve this potential vulnerability as a precaution as of 3.8.20 and 3.9.7 BlueX software releases.

RAM® 9000, RAM 6000, SN 6000 and M, A and R Series

The affected bash shell is running as part of the system process, deep in the runtime environment. User access to system services (GUI, SSH, CLI, etc.) are protected by username/password authentication. Any attempt to access potentially vulnerable systems would first require the login information of the unit. Due to the authentication process, these systems are not externally vulnerable to the Shellshock bash exploit. Release 3.19 and 4.19 provide an update to the latest bash executable. A patch will also be made available to update older units with the latest bash executable.

We advise all customers to follow best practices with password maintenance to maintain a high level of security. For any additional questions, please contact Red Lion Technical Support.