Support Bulletin

Bash/Shellshock Exploit Vulnerability Update N1031-01

November 5, 2014

Some products sold and/or supported by VeEX may be affected by the Bash/Shellshock vulnerability. This bulletin lists the status of related products, available fixes and recommendations. It is recommended to keep all products updated to the latest OS versions packages available.

In 2014 a serious security vulnerability known as the Bash (GNU Bourne Again Shell) or Shellshock bug was identified. It affects all UNIX-based operating systems, including all versions of Linux. Bash is an sh-compatible shell designed to conform to IEEE POSIX P1003.2/ISO 9945.2 Shell and Tools standard, so most sh scripts can be run by Bash without modification. GNU Bash versions up to 4.3, process trailing strings after function definitions in the values of environment variables. This vulnerability allows malicious code execution within the Bash shell (commonly accessed through a Command Prompt on a PC or Mac's Terminal application) up to and including compromising an operating system. An attacker can provide specially-crafted environment variables containing arbitrary commands that will be executed on vulnerable systems under certain conditions.

 VeEX has addressed the Bash vulnerability by adding the fix to all affected products. A system update may be required.

VeEX Product	OS & Shell	Status	Recommended actions	Where to go?
UX400 Platform	Ubuntu Linux 10.4, Bash shell	Vulnerable but low risk (fixed)	Upgrade to UX400 RootFS 1.2.6 or latest	CustomerCare@veexinc.com
RealWorx	Red Hat Linux 5.5, Bash shell	Vulnerable (fixed)	Contact Customer Care to coordinate the upgrade to the latest version 5.2.13-1	CustomerCare@veexinc.com
RealGATE	Red Hat Linux 5.5, Bash shell	Vulnerable (fixed)	Contact Customer Care to coordinate the upgrade to the latest Bash version	CustomerCare@veexinc.com
VeSion	Windows Server	Not Affected	No action required	
CX180R RPM	Windows Server	Not Affected	No action required	
CX180F	Windows Server	Not Affected	No action required	
R300	Windows Server	Not Affected	No action required	
V100-series	Linux. Busybox shell	Not Affected	No action required	
V300-series	Linux. Busybox shell	Not Affected	No action required	
RXT-1200	Linux. Busybox shell	Not Affected	No action required	
CM-series	Windows CE	Not Affected	No action required	
AT-series	Linux. Busybox shell	Not Affected	No action required	
MTT-series	pSOS RTOS	Not Affected	No action required	

Although no other products are considered affected, an investigation into all VeEX and Sunrise Telecom products is ongoing. This document would be updated if any additional information or patches are made available.

It is also recommended that customer-owned Linux-based servers being used to host any other VeEX or Sunrise Telecom software shall be updated to the latest Linux version containing the Bash/Shellshock fix. Please identify the Linux version

running on such servers and research the options available via their website or by contacting the manufacturer, to obtain the latest patches available.

VeEX's priority is the security of our customers' network. In the event that a vulnerability is found within any of VeEX's or Sunrise Telecom's server software, we work closely with the OS supplier. VeEX would only disclose product vulnerabilities when a workaround, patch or fix is available, to avoid informing the hacker community that our products may be a suitable target, which could put our customers at a greater risk.

For more up-to-date information, please visit the Support section at www.veexinc.com or contact us at customercare@veexinc.com