1601 S. MoPac Expwy, Suite 100
Austin, Texas 78746
(P) +1 512 347 9300
www.lifesize.com

Lifesize Shellshock (CVE-2014-6271 and CVE-2014-7169) Status/Response
9/29/14 – 7:15pm CDT

The "Shellshock" vulnerability is in the command line interface ("bash") used on most Linux systems. All of our systems running Linux do have versions of bash that are vulnerable, but we have not found any paths for unauthorized users to access bash.

We have run several vulnerability scanners and have not found any of our products to show as vulnerable.

NOTE: You can get these scanners to show portions of UVC as vulnerable if you give the scanner your administrator login credentials.

We have tested the following Lifesize products:

- Icon Series
- 220 Series Endpoints
- UVC platform and all applications
- NOTE: bash is an application provided by the operating system. In cases of mobile or desktop clients, response to this vulnerability is the responsibility of the operating system – Apple iOS, Mac OSX, or Google Android. Windows does not run bash.

We have used the following scanners:

- https://suite.websecurify.com/apps/shellshock/
- http://milankragujevic.com/projects/shellshock/
- Nessus (by Tenable)

Please feel free to use the scanners listed above or any others to verify your Lifesize systems are not vulnerable.

There are additional recommended tests on the Internet that apply to cases where the user has direct access to bash. None of our products provide bash access to either the user or administrator.

We will work to update our bash versions, but do not believe that any of our products are at risk at this point. We will also continue to scan and test our products as the tools for detecting this issue evolve.

Mike Burkett
Director, Customer Advocacy
mburkett@lifesize.com