

## **Lifesize Poodle (CVE-2014-3566) Status/Response**

10/27/14 – 8:35am CDT

The “Poodle” vulnerability is an attack on the SSLv3 protocol used by some systems for secure communications, primarily encountered by users when accessing web sites from their browser.

All of the Lifesize systems we have tested are susceptible to this vulnerability and we are working to provide software updates that will correct this issue.

For now, we recommend that you address the issue by fixing your browser as outlined on the following website – <https://zmap.io/ssl3/browsers.html>

We will update this notice later this week with specific product versions containing the fix for this vulnerability.

As a consistent reminder, we recommend that you deploy Lifesize equipment such that the web interface ports (80/443) and ssh ports (22) are not accessible to the public internet. You should be able to configure this via your firewall settings. You should only expose the web interface for products where people outside your organization need access to it.

Please feel free to contact us with any questions or concerns.

Mike Burkett  
Director, Customer Advocacy  
[mburkett@lifesize.com](mailto:mburkett@lifesize.com)