Poodle: SSLv3 Vulnerability - Frequently Asked Questions

Q. What does POODLE: SSL V3 vulnerability mean? What are the steps that I should perform from the client side to access CenturyLink systems?

A. • Reference for all browser changes - "POODLE Disabling SSLv3 Support in Browsers"

Refer to the following link to learn more - https://zmap.io/sslv3/browsers.html

• Red Hat security advisory - "POODLE: SSL V3 vulnerability CVE - 2014 - 3566".

Refer to the following link to learn more - https://access.redhat.com/articles/1232123

• Open SSL security advisory - "This Poodle Bites: Exploiting the SSL 3.0 Fallback" September 2014.

Refer to the following link to learn more - https://www.openssl.org/~bodo/ssl-poodle.pdf

• Microsoft security advisory 300-9008 - "Vulnerability in SSL 3.0 Could Allow Information Disclosure".

Refer to the following link to learn more https://technet.microsoft.com/en-us/library/security/3009008.aspx

Q. As we are utilizing the Production URL's for sending XML orders, do we need to utilize a different mode of transport in sending e-bonded orders?

A. No, you will not be required to utilize a different mode of transport for sending e-bonded orders. There is NO impact to the IMA XML transmitted orders to https://ixgprod.ordering.centurylink.com:443/imaOrder/order via the Soap mode of transport.

Background:

CenturyLink is following the Industry Wide Security advisory to just disable one of the many web security Protocols we all currently use.

To secure data that is being sent between applications across an entrusted network, such as the Internet, we need security protocols which establish trust and authentication. Transport Layer Security (TLS) which uses Secure Socket Layer (SSL) is one of the most widely recognized security protocols which has always provided secure HTTP (HTTPS) for Internet transactions between Web browsers and Web servers. TLS/SSL enables server authentication, client authentication, data encryption, and data integrity over networks such as the Internet for web services. From the beginning of IMA, we have all used TLS/SSL as it was defined as part of the TCIF standards to secure our applications.

When the TLS standards Internet Engineering Task Force (IETF) started, they adopted SSL 3.0 from Netscape as their starting point. That became the TLS protocol version.0.

(Reminder: SSLv3.0/SSL was developed by Netscape Communications Corporation in 1994 to secure transactions over the World Wide Web.)

Poodle: SSLv3 Vulnerability - Frequently Asked Questions

Although there are some slight differences between the 1998 SSL 3.0 and the newer versions, TLS still includes SSL but provides a newer SSL version. The vulnerability in the SSLv3 protocol, commonly referred to as 'POODLE' (which stands for Padding Oracle On Downgraded Legacy Encryption), only affects the oldest TLS version of encryption, specifically SSLv3, but does not affect the newer encryption mechanism known as TLS/SSL.

On system “startup” each day, there are many TLS versions which are enabled for talking to another company’s server. The two servers must negotiate on a single common TLS/SSL security protocol, such as, SSLv3, TLS/SSL 1.0, 1.1, 1.2, which are all enabled in our web server security toolkits. In this case, we are just being asked to turn off the TLS “SSLv3” option from 1998 and no longer support this 18 year old version of TLS. We will then support only the newer TLS/SSL versions 1.0, 1.1, and 1.2.

Q. Is the SSLv3 access already been shut off on test environment?

A. The IMA-SATE and MTG Test environments for XML have been updated to disable SSLv3 protocol. Only TLS/SSL protocol is now supported in these test environments.

If you wish to test in either of these environments prior to December 14, 2014, CenturyLink is requesting that you send an email to ITCOMM@centurylink.com identifying the planned test date. CenturyLink will then monitor testing to provide you a response as to the success of your testing effort.