Customer Advisory

POODLE Remediation: Secure Sockets Layer (SSL) Change Affecting Inovisworks™ Electronic Data Interchange

Details

The OpenText GXS Customer Service Organization is dedicated to ensuring that you are proactively informed of any changes to our network. As part of our ongoing efforts to strengthen the configuration of the GXS network and reduce our vulnerability to POODLE attacks, OpenText GXS will disable Secure Sockets Layer (SSL) version 3 and earlier to prevent it from being used to connect to our Inovisworks service through one of the GXS communication gateways listed below. Instead, OpenText will use Transport Layer Security (TLS), which is the recommended protocol version to safeguard against POODLE attacks.

We are providing you with this Customer Advisory to ensure affected users have an opportunity to either modify the method used to connect to our Inovisworks service or work with OpenText GXS to allow for alternatives so that the critical exchange of electronic business documents with your trading community is not interrupted.

Systems Affected

Customers and trading partners who establish an Inovisworks message exchange connection through one of the following GXS communication gateways may be affected:

Inovisworks Core VAN
ftpssl.gateway.inovisworks.net
https://pipeline.gateway.inovisworks.net
https://pipeline.harbinger.net

Inovisworks Core VAN Biz
https://as2.gateway.inovisworks.net/as2
https://as2.gateway.inovisworks.net/http

Inovisworks MS OS2.0 Biz PROD
ftpssl.gateway.inovisworks.net
https://visibility.inovis.com/dataquality/xclient/
https://as2.gateway.inovisworks.net/inovis/as2
https://as2.gateway.inovisworks.net/inovis/http

Inovisworks MS OS2.0 Biz UAT
ftpssl.gateway.inovisworks.net
https://as2.gateway.inovisworks.net/inovis/bizsim/as2
https://as2.gateway.inovisworks.net/inovis/bizsim/http

GXS Active Catalogue

Production

https://catalogue.gxs.com/QRSGUI/services/ItemWebService
https://catalogue.gxs.com/QRSGUI/services/ProductWebService
https://catalogue.gxs.com/QRSGUI/services/SelcodeWebService
https://catalogue.gxs.com/QRSGUI/services/AccountWebService

Pre-production

https://cataloguedemo.gxs.com/QRSGUI/services/ItemWebService
https://cataloguedemo.gxs.com/QRSGUI/services/ProductWebService
https://cataloguedemo.gxs.com/QRSGUI/services/SelcodeWebService
https://cataloguedemo.gxs.com/QRSGUI/services/AccountWebService

Web Client

https://catalogue.gxs.com/QRSGUI/jsf/login/login.jspx (Production)
https://cataloguedemo.gxs.com/QRSGUI/jsf/login/login.jspx (Pre-production)

DQC/Active Intelligence

LSPROD (shared)
https://visibility.inovis.com/dataquality/xclient

Prod2 (shared)
https://visibilitycl2.ms.gxs.com/sdataquality/xclient

Gridtalk (Rosettanet)

Implementation
https://rosettanet-imp.inovis.com/gridtalk/b2bi/rosettanet

Staging
https://rosettanet-stage.inovis.com/gridtalk/b2bi/rosettanet

Production
https://rosettanet-live.inovis.com/gridtalk/b2bi/rosettanet

Impact

Starting **November 15, 2015**, OpenText GXS will no longer support Secure Sockets Layer (SSL) to establish an Inovisworks message exchange connection with GXS communication gateways. Customers and trading partners will need to use TLS to establish an Inovisworks message exchange connection with certain GXS communication gateways (see Systems Affected above).

Note: Customers are responsible to notify their trading partners of any action required to prepare them for the upcoming POODLE remediation.

Solution

To prepare for this change and help prevent any disruption in service, customers should proactively update their communication software to ensure that it supports TLS in fallback mode (TLS 1.2, 1.1, and 1.0). Please ensure that TLS 1.2, 1.1 and 1.0 are enabled as TLS 1.0 may be required to establish an Inovisworks message exchange connection with certain GXS communication gateways.

Beginning **November 1, 2015**, customers will be able to test their ability to connect to the Inovisworks service in a pre-production environment. OpenText strongly recommends that customers test their connection prior to the November 15th rollover date. If you experience difficulties connecting to our services in the pre-production environment, your organization will need to be added to our exception listing (see below).

Note: If you use a third-party software package to connect to our services, OpenText recommends that you contact your software provider as soon as possible to ensure TLS is supported and you can safely disable SSL.

Exception Listing

Although OpenText recommends disabling SSL as the most effective way to address the POODLE threat, we understand that not all customers can support TLS. If you are unable to support TLS, GXS has established an exception listing that will allow customers to continue to access the GXS network using SSL. In order to enable your continued use of SSL, you will be required to visit our website to add your company to our exception listing.

More Information

For more information, refer to the FAQ or contact Cloud Support Services.