OPENTEXT™

POODLE Vulnerability

Frequently Asked Questions

How do I use this document?

This FAQ provides answers to some of the most frequently asked questions by our customers regarding the POODLE vulnerability. This is a living document and will be updated regularly at http://techsupport.gxs.com/.

What is POODLE?

POODLE is an acronym for **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption. The security issue is exactly what the name suggests, a protocol downgrade that allows exploits on an outdated form of encryption. The issue came to the world's attention when Google released a paper called This POODLE Bites: Exploiting The SSL 3.0 Fallback.

How does POODLE work?

POODLE allows an attacker to perform a *man-in-the-middle* attack which may force a connection to "fallback" to Secure Sockets Layer (SSL) version 3.0, making it possible for an attacker to obtain sensitive user data. The data at risk of being exposed can vary based on the type of SSL connectivity enabled.

This vulnerability is rated as Medium. This means that the issue provides an opportunity for an attacker to compromise the confidentiality, integrity, and/or availability of data elements, but requires one or more pre-conditions to exist. A POODLE attack is extremely difficult to execute and requires over 250 transaction attempts to reveal a single byte of data.

What is OpenText doing to protect customers?

OpenText security experts are currently analyzing the risks associated with POODLE. Where necessary, OpenText will disable SSL version 3 and earlier to prevent it from being used to access GXS communication gateways. Instead, OpenText will use Transport Layer Security (TLS), which is the recommended protocol version to safeguard against POODLE attacks.

How does this affect me?

Any service that supports Secure Sockets Layer (SSL) version 3 (SSLv3) may be exploited so that an attacker can decrypt secure sessions, potentially revealing user data.

A connection is only susceptible to a POODLE attack if both the sender and receiver support SSLv3. If you have already disabled SSLv3, you are not affected by the issue documented above. OpenText recommends that you contact your internal application administrator or software provider to ensure you are using TLS 1.0 or later (with SSLv3 disabled) to connect to our services.

What do I need to do?

OpenText will update the protocol on affected communication gateways in phases. Remediation plans are still being finalized and details on roll-over dates will be communicated shortly. Customers will be given reasonable notification of changes before the planned roll-over dates.

In the meantime, customers should proactively ensure that their communication software supports TLS in fallback mode (TLS 1.2, 1.1, and 1.0). If your use case allows, OpenText recommends that you disable SSL immediately. Please contact your software provider if you have any questions on how to disable SSL.

What browsers are affected by POODLE?

For browser based applications, any web browser that makes use of SSLv3 is at risk. Although the majority of modern web browsers (Chrome, Firefox, Safari, and Internet Explorer 9+) use TLS 1.0 or later, legacy browsers such as Internet Explorer 6 only support SSLv3. This means that users who are utilizing older PCs and browser versions may be impacted by the POODLE vulnerability.

What happens to my account if I try to access OpenText services without updating my browser?

Although your account will not be shut down, the connection will be refused and you will be unable to access OpenText services.

What connection methods could be susceptible to POODLE?

OpenText Information Security is conducting an analysis to determine the risk that POODLE represents to the various communications protocols used to connect to OpenText services. The list of communications protocols that make use of the security capabilities of SSL include:

- HTTPs
- FTPs
- AS2
- RosettaNet
- OFTP
- MQ
- AS3

If you or your trading partner(s) use any of the communications protocols listed above, there is no immediate need for concern. OpenText is conducting a risk analysis on each protocol to

determine which protocols require SSL to be disabled. Affected customers will be given reasonable notification of changes before the planned roll-over dates (normally 60 days).

How do I disable SSLv3?

Browsers:
There are many resources available on the internet that provide instructions on how to disable SSLv3 support in browsers. An example would be https://zmap.io/sslv3/browsers.html.

Connection Software:
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.

How do I know if my service(s) are affected by the remediation plan?

The customer advisories for each communication protocol include lists of the gateway URLS that make use of the security capabilities of SSL and are affected by the remediation plan. To review the lists of gateway URLs, please visit our website and download the advisory for your communication protocol.

When will SSL be turned off for my communication gateway?

OpenText will update the protocol on affected communication gateways in phases. Remediation plans are still being finalized and details on roll-over dates will be communicated shortly. To review the schedule for communication protocols that have already been remediated, please visit our website.

My system cannot support Transport Layer Security (TLS). What do I do?

Although OpenText recommends disabling SSL as the most effective way to address the POODLE threat, we understand that not all customers can support Transport Layer Security (TLS). If you are unable to support TLS, OpenText 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

What about my trading partners?

As communication gateways are remediated, customers and trading partners will need to use TLS to establish a message exchange connection with OpenText GXS communication gateways. Customers are responsible to notify their trading partners of any action required to prepare them for the upcoming POODLE remediation.

If you have a trading partner who connects directly to OpenText services and cannot support Transport Layer Security (TLS) and wish to be added to the exception listing, they will need to provide OpenText with their IP address.

Who should I contact for further information?

If you have any questions or need additional assistance, you may contact your support organization using the contact information provided to you or you may visit the **OpenText website** for worldwide contact information.

OPENTEXT™

About OpenText

OpenText provides Enterprise Information Management software that helps companies of all sizes and industries to manage, secure and leverage their unstructured business information, either in their data center or in the cloud. Over 50,000 companies already use OpenText solutions to unleash the power of their information. To learn more about OpenText (NASDAQ: OTEX; TSX: OTC), please visit www.opentext.com.

www.opentext.com

NORTH AMERICA +800 499 6544 • UNITED STATES +1 847 267 9330 • GERMANY +49 89 4629 0

UNITED KINGDOM +44 0 1189 848 000 • AUSTRALIA +61 2 9026 3400