
GXS communication gateways may be vulnerable to the Padding Oracle on Downloaded Legacy Encryption (POODLE) bug.

Please review this advisory to determine whether your site is vulnerable and learn how to mitigate this vulnerability.

Systems Affected

- All GXS communication gateways that enable subscribers to send or receive files, through a Secure Sockets Layer (SSL) communication protocol.

Details

The protocol used by GXS communication gateways to establish a SSL connection may be vulnerable to the POODLE bug (CVE-2014-3566). POODLE attacks are extremely difficult to execute and require over 250 transaction attempts to reveal a single byte of data.

Impact

Any service that supports SSL version 3 (SSLv3) can be exploited so that an attacker can decrypt secure sessions, potentially revealing passwords and other private information. A connection is only susceptible if both the sender and receiver support SSLv3.

Note: If you already use Transport Layer Security (TLS) 1.0 or later to access GXS communication gateways, you are not affected by the issue documented in this Security Advisory. Contact your internal application administrator or software provider to ensure you are using TLS 1.0 or later to connect to our services.

Solution

OpenText will disable SSL to prevent it from being used to access GXS communication gateways. Instead, OpenText will use TLS 1.0, which is a more recent protocol that is not affected by the POODLE bug. Remediation plans are being finalized and will be announced shortly.

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).

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.

More Information

For more information, refer to the [FAQ](#) or contact [GXS Customer Support](#).

Copyright ©2015 Open Text Corporation. All Rights Reserved. OpenText is a trademark or registered trademark of Open Text SA and/or Open Text ULC. The list of trademarks is not exhaustive of other trademarks, registered trademarks, product names, company names, brands and service names mentioned herein are property of Open Text SA or other respective owners. All rights reserved. For more information, visit: <http://www.opentext.com/2/global/site-copyright>.

www.gxs.com
www.opentext.com



[Click here](#) to open this email in your browser | [Click here](#) to unsubscribe from OpenText | GXS emails

© Copyright 2014 OpenText Corporation and/or its subsidiaries. All Rights Reserved | [Privacy Policy](#)
GXS, 9711 Washingtonian Boulevard, Gaithersburg, MD 20878 | Tel: +1 301-340-4000 Fax: +1 301-340-5299 www.gxs.com