OPENTEXT | GXS

Avis de sécurité

Les passerelles de communication GXS pourraient être vulnérables au bug POODLE (Padding Oracle on Downloaded Legacy Encryption).

Veuillez lire cet avis afin de déterminer si votre site est vulnérable et savoir comment atténuer cette vulnérabilité.

Systèmes concernés

- Toutes les passerelles de communication GXS permettant aux abonnés d'envoyer ou de recevoir des fichiers, par le biais du protocole de communication SSL (Secure Sockets Layer).

Détails

Le protocole utilisé par les passerelles de communication GXS pour établir une connexion SSL pourraient être vulnérable au bug POODLE (CVE-2014-3566). Les attaques POODLE sont extrêmement difficiles à exécuter et nécessitent plus de 250 tentatives de transaction pour révéler un seul octet de données.

Impact

Tout service qui prend en charge SSL version 3 (SSLv3) peut être exploité par un attaquant pour décrypter des sessions sécurisées, risquant ainsi d'exposer des mots de passe et d'autres informations privées. Une connexion n'est vulnérable que si l'émetteur et le récepteur supportent SSLv3.

Remarque : Si vous utilisez déjà TLS (Transport Layer Security) 1.0 ou une version ultérieure pour accéder aux passerelles de communication GXS, vous n'êtes pas concerné par le problème décrit dans cet Avis de Sécurité. Contactez le responsable interne de vos applications ou votre fournisseur de logiciels pour vérifier que vous utilisez bien TLS 1.0 ou une version ultérieure pour vous connecter à nos services.

Solution

OpenText désactivera la couche SSL pour éviter qu'elle ne soit utilisée pour accéder aux passerelles de communication GXS. OpenText utilisera à la place TLS 1.0, un protocole plus récent qui n'est pas affecté par le bug POODLE. Des plans de correction sont en cours de finalisation et seront annoncés sous peu.

Pour se préparer à ce changement et éviter toute perturbation des services, les clients sont invités à mettre à jour de manière proactive leur logiciel de communication afin de s'assurer qu'il supporte TLS en mode de secours (TLS 1.2, 1.1 et 1.0).

Remarque : Si vous utilisez un logiciel tiers pour vous connecter à nos services, OpenText vous recommande de contacter votre fournisseur de logiciel dès que possible pour vérifier que TLS est bien pris en charge et que vous pouvez désactiver SSL en toute sécurité.

Plus d'informations

Pour plus d'informations, reportez-vous à la FAQ ou contactez GXS Customer Support.