OPENTEXT™

Vulnérabilité POODLE

Foire aux questions

Comment puis-je utiliser ce document ?

Cette FAQ fournit des réponses à certaines des questions les plus fréquemment posées par nos clients concernant la vulnérabilité POODLE. Il s'agit d'un document vivant qui sera mis à jour régulièrement sur http://techsupport.gxs.com/.

Qu'est-ce que POODLE ?

POODLE est un acronyme pour **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption. Le problème de sécurité qu'il soulève correspond exactement à ce que son nom indique, à savoir le passage à une version antérieure d'un protocole qui permet d'exploiter une forme de cryptage obsolète. La question a été portée à l'attention générale lorsque Google a publié un document intitulé This POODLE Bites: Exploiting The SSL 3.0 Fallback.

Comment fonctionne POODLE ?

POODLE permet à un attaquant d'exécuter une attaque *dite de l'homme du milieu* qui peut forcer une connexion à « se replier » sur la version 3.0 de SSL (Secure Sockets Layer), ce qui lui permet d'obtenir des données confidentielles de l'utilisateur. Les données qui risquent d'être exposées peuvent varier en fonction du type de connectivité SSL activé.

Cette vulnérabilité est classée en tant que vulnérabilité moyenne. Ceci signifie qu'elle offre une occasion pour un attaquant de compromettre la confidentialité, l'intégrité et/ou la disponibilité des éléments de données mais nécessite une ou plusieurs conditions préalables pour exister. Une attaque POODLE est extrêmement difficile à exécuter et nécessite plus de 250 tentatives de transaction pour révéler un seul octet de données.

Que fait OpenText pour protéger ses clients ?

Les spécialistes de la sécurité d'OpenText sont actuellement en train d'analyser les risques associés à POODLE. Le cas échéant, OpenText désactivera le protocole SSL, versions 3 et précédentes, pour éviter qu'il ne soit utilisé pour accéder aux passerelles de communication GXS. OpenText va le remplacer par TLS (Transport Layer Security), qui est la version du protocole recommandée pour se prémunir contre les attaques POODLE.

En quoi suis-je concerné ?

Tout service qui prend en charge SSL (Secure Sockets Layer) version 3 (SSLv3) peut être exploité par un attaquant pour décrypter des sessions sécurisées et risque donc de révéler les données de l'utilisateur.

Une connexion ne peut être soumise à une attaque POODLE que si l'émetteur et le récepteur prennent en charge SSLv3. Si vous avez déjà désactivé SSLv3, vous n'êtes pas concerné par le problème décrit ci-dessus. OpenText vous recommande de contacter le responsable interne

de vos applications ou votre fournisseur de logiciels pour vérifier que vous utilisez bien TLS 1.0 ou une version ultérieure (avec SSLv3 désactivé) pour vous connecter à nos services.

Que dois-je faire ?

OpenText va progressivement mettre à jour le protocole sur les passerelles de communication affectées. Les plans de correction sont en cours de finalisation et le détail des dates de déploiement sera communiqué sous peu. Les clients seront avertis des changements avant les dates de déploiement planifiées et dans un délai raisonnable.

En attendant, les clients doivent s'assurer que leur logiciel de communication prend en charge TLS en mode de secours (TLS 1.2, 1.1 et 1.0). Si votre configuration le permet, OpenText vous recommande de désactiver SSL immédiatement. Veuillez contacter votre fournisseur de logiciels si vous avez des questions quant à la façon de désactiver SSL.

Quels navigateurs sont touchés par POODLE ?

Pour les applications basées sur un navigateur, tout navigateur Web qui utilise SSLv3 présente un risque. Si la majorité des navigateurs Web modernes (Chrome, Firefox, Safari et Internet Explorer 9+) utilisent TLS 1.0 ou une version ultérieure, les anciens navigateurs tels qu'Internet Explorer 6 prennent uniquement en charge SSLv3. Par conséquent, les utilisateurs qui se servent de PC anciens et d'anciennes versions de navigateur peuvent être affectés par la vulnérabilité POODLE.

Qu'advient-il de mon compte si je tente d'accéder aux services OpenText sans mettre à jour mon navigateur ?

Votre compte ne sera pas fermé, mais la connexion sera refusée et il vous sera impossible d'accéder aux services OpenText.

Quelles méthodes de connexion peuvent être vulnérables face à POODLE ?

OpenText Information Security effectue actuellement une analyse visant à déterminer le risque représenté par POODLE pour les différents protocoles de communication utilisés pour se connecter aux services OpenText. La liste des protocoles de communication qui utilisent les capacités de sécurité de SSL inclut :

- HTTPS
- FTPs
- AS2
- RosettaNet
- OFTP
- MQ

- AS3

Si vous ou vos partenaires commerciaux utilisez l'un des protocoles de communication mentionnés ci-dessus, il n'y a pas d'inquiétude à avoir pour le moment. OpenText procède à une analyse de risque sur chaque protocole afin de déterminer quels protocoles SSL doivent être désactivés. Les clients concernés seront avertis des changements avant les dates de déploiement planifiées et dans un délai raisonnable (normalement 60 jours).

Comment désactiver SSLv3 ?

Navigateurs :
De nombreuses ressources sur Internet fournissent des instructions sur la façon de désactiver la prise en charge SSLv3 dans les navigateurs. Par exemple : https://zmap.io/sslv3/browsers.html.

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

Comment savoir si certains de mes services sont affectés par le plan de correction ?

Les avis à la clientèle relatifs à chaque protocole de communication comprennent une liste des adresses URL des passerelles qui utilisent les capacités de sécurité de SSL et qui sont concernées par le plan de correction. Pour consulter les listes des adresses URL des passerelles, veuillez consulter notre site Web et télécharger l'avis relatif à votre protocole de communication.

En ce qui concerne ma passerelle de communication, quand SSL sera-t-il désactivé ?

OpenText va progressivement mettre à jour le protocole sur les passerelles de communication affectées. Les plans de correction sont en cours de finalisation et le détail des dates de déploiement sera communiqué sous peu. Pour connaître le calendrier concernant les protocoles de communication déjà corrigés, veuillez consulter notre site Web.

Mon système ne prend pas en charge le protocole TLS (Transport Layer Security). Que dois-je faire ?

Bien qu'OpenText recommande de désactiver le protocole SSL pour lutter le plus efficacement possible contre la menace POODLE, nous sommes conscients que certains clients ne peuvent pas prendre en charge le protocole TLS (Transport Layer Security). Si vous ne pouvez pas prendre en charge le protocole TLS, OpenText GXS a établi une liste des exceptions qui permettra aux clients qui y figurent de continuer à accéder au réseau GXS à l'aide du protocole SSL. Pour continuer à utiliser le protocole SSL, veuillez consulter notre site Web afin d'ajouter votre société à notre liste des exceptions.

Qu'advient-il de mes partenaires commerciaux ?

À mesure que les passerelles de communication sont corrigées, les clients et partenaires commerciaux devront utiliser le protocole TLS pour établir une connexion d'échange de messages avec les passerelles de communication OpenText GXS. Il revient aux clients d'informer leurs partenaires commerciaux de toute action requise en vue de les préparer aux plans de lutte à venir contre les attaques POODLE.

Si l'un de vos partenaires commerciaux se connecte directement aux services OpenText mais ne peut pas prendre en charge le protocole TLS (Transport Layer Security) et souhaite figurer sur la liste des exceptions, il devra fournir son adresse IP à OpenText.

Qui dois-je contacter pour plus d'informations ?

Si vous avez des questions ou si vous avez besoin d'une assistance supplémentaire, vous pouvez contacter votre organisme de soutien en utilisant les informations de contact qui vous ont été fournies ou bien vous pouvez consulter le **site Web OpenText** pour obtenir des informations de contact dans le monde entier.

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

AMÉRIQUE DU NORD +800 499 6544 • ÉTATS-UNIS +1 847 267 9330 • ALLEMAGNE +49 89 4629 0

ROYAUME-UNI +44 0 1189 848 000 •AUSTRALIE +61 2 9026 3400