OPENTEXT™

Vulnerabilidade POODLE

Perguntas frequentes

Como devo utilizar este documento?

Este documento fornece respostas para algumas das perguntas frequentes feitas pelos nossos clientes sobre a vulnerabilidade POODLE. Este documento é dinâmico e será atualizado regularmente no site http://techsupport.gxs.com/.

O que significa POODLE?

POODLE é o acrônimo de **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption (algo como "Defesa do Oracle em criptografia existente desatualizada"). A questão da segurança é exatamente o que o nome sugere. Uma desatualização de protocolo que permite a exploração em uma forma ultrapassada de criptografia. O problema veio à atenção do mundo quando o Google divulgou um documento chamado Este POODLE morde [This POODLE Bites]: Explorando o Fallback do SSL 3.0 [Exploiting The SSL 3.0 Fallback].

Como o POODLE funciona?

O POODLE permite que um invasor execute um ataque a intermediários, que pode fazer com que uma conexão volte ("fallback") para o protocolo Secure Sockets Layer (SSL) versão 3.0, possibilitando que um invasor capture dados confidenciais do usuário. Os dados em risco de serem expostos podem variar com base no tipo de conectividade SSL habilitada.

Esta vulnerabilidade é classificada como Média. Isso significa que a questão oferece uma oportunidade para um invasor comprometer a confidencialidade, integridade e/ou disponibilidade de elementos de dados, mas exige a existência de um ou mais pré-requisitos. É extremamente difícil executar um ataque POODLE, sendo necessário realizar mais de 250 tentativas de transações para revelar um único byte de dados.

O que a OpenText está fazendo para proteger os clientes?

Os especialistas em segurança da OpenText estão atualmente analisando os riscos associados à vulnerabilidade POODLE. Sempre que necessário, a OpenText desabilitará o SSL versão 3 e anteriores para evitar que sejam utilizados para acessar os gateways de comunicação GXS. Em seu lugar, a OpenText utilizará o protocolo de Segurança da Camada de Transporte (TLS, Transport Layer Security), que é a versão de protocolo recomendada para proteção contra ataques POODLE.

Como isso me afeta?

Qualquer serviço compatível com o protocolo Secure Sockets Layer (SSL) versão 3 (SSLv3) pode ser explorado, permitindo que um invasor descriptografe sessões seguras, com o potencial de revelar dados do usuário.

Uma conexão é suscetível a um ataque POODLE apenas se o remetente e o receptor forem compatíveis com SSLv3. Se o SSLv3 já tiver sido desabilitado, o seu sistema não será afetado pela situação documentada acima. A OpenText recomenda que você entre em contato com o seu administrador de aplicativos internos ou provedor de software para verificar se está usando o TLS 1.0 ou posterior (com o SSLv3 desabilitado) para se conectar aos nossos serviços.

O que eu preciso fazer?

A OpenText atualizará, por etapas, o protocolo nos gateways de comunicação afetados. Os planos de correção ainda estão sendo concluídos e os detalhes sobre as datas de implantação serão comunicados em breve. Os clientes serão notificados em tempo hábil com relação às alterações antes das datas planejadas de implantação.

Enquanto isso, os clientes devem garantir proativamente que o software de comunicação seja compatível com o TLS em modo fallback (TLS 1.2, 1.1 e 1.0). Se o seu caso de uso permitir, a OpenText recomenda desabilitar o SSL imediatamente. Se você tiver alguma dúvida sobre como desabilitar o SSL, entre em contato com o seu provedor de software.

Quais navegadores são afetados pelo POODLE?

Para aplicativos com base em navegador, qualquer navegador que utilize o SSLv3 pode ser afetado. Embora a maioria dos navegadores modernos (Chrome, Firefox, Safari e Internet Explorer 9+) utilize TLS 1.0 ou posterior, navegadores antigos, como Internet Explorer 6, são compatíveis apenas com SSLv3. Isso significa que os usuários que utilizam PCs mais antigos e versões de navegadores mais antigas podem ser afetados pela vulnerabilidade POODLE.

O que acontece à minha conta se eu tentar acessar os serviços da OpenText sem atualizar o meu navegador?

A sua conta não será fechada, mas a conexão será negada e você não conseguirá acessar os serviços da OpenText.

Quais métodos de conexão poderiam ser suscetíveis ao POODLE?

A OpenText Information Security está realizando uma análise para determinar o risco que o POODLE representa aos diferentes protocolos de comunicação usados para conexão aos serviços da OpenText. A lista de protocolos de comunicação que utilizam os recursos de segurança do SSL inclui:

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

Se você ou seus parceiros comerciais utilizam qualquer um dos protocolos de comunicação listados acima, por enquanto está tudo sob controle. A OpenText está realizando uma análise de risco sobre cada protocolo para determinar quais protocolos exigem que o SSL seja desabilitado. Os clientes afetados receberão notificações em tempo hábil sobre as alterações antes das datas planejadas de implantação (normalmente 60 dias).

Como faço para desabilitar o SSLv3?

Navegadores:
Há muitos recursos disponíveis na internet que fornecem instruções sobre como desabilitar a compatibilidade com o SSLv3 nos navegadores. Um exemplo seria o site https://zmap.io/sslv3/browsers.html.

Software de conexão:
Se você utiliza um pacote de software de terceiros para conectar aos nossos serviços, a OpenText recomenda que entre em contato com o seu provedor de software o quanto antes para garantir que o TLS seja compatível e que possa desabilitar o SSL com segurança.

Como posso saber se os meus serviços são afetados pelo plano de correção?

O arquivo de assessoria ao cliente de cada protocolo de comunicação inclui listas dos URLs de gateways que utilizam os recursos de segurança do SSL afetados pelo plano de correção. Para verificar as listas de URLs de gateways, acesse o nosso site e baixe o arquivo do seu protocolo de comunicação.

Quando o SSL do meu gateway de comunicação será desativado?

A OpenText atualizará, por etapas, o protocolo nos gateways de comunicação afetados. Os planos de correção ainda estão sendo concluídos e detalhes sobre as datas de implantação serão comunicados em breve. Para verificar a programação dos protocolos de comunicação que já foram corrigidos, acesse o nosso site.

Meu sistema não é compatível com o protocolo de Segurança da Camada de Transporte (TLS, Transport Layer Security). O que devo fazer?

Embora a OpenText recomende desabilitar o SSL como a maneira mais eficaz para lidar com a ameaça da falha POODLE, entendemos que nem todos os clientes podem ser ter a possibilidade de utilizar TLS. Se você não puder utilizar TLS, a GXS da OpenText estabeleceu uma lista de exceções que permitirá que os clientes continuem a acessar a rede GXS usando o SSL. Para permitir o uso continuado do SSL, será necessário acessar o nosso site para adicionar a sua empresa à nossa lista de exceções.

E os meus parceiros comerciais?

À medida que os gateways de comunicação forem corrigidos, os clientes e parceiros comerciais precisarão usar o TLS para estabelecer uma conexão de troca de mensagens com os gateways de comunicação GXS da OpenText. Os clientes são responsáveis por notificar seus parceiros comerciais sobre qualquer ação necessária para prepará-los para a futura correção da falha POODLE.

Se você tiver um parceiro comercial que se conecte diretamente aos serviços da OpenText, sem compatibilidade com o Transport Layer Security (TLS) e gostaria de ser adicionado à lista de exceções, ele precisará fornecer os endereços de IP à OpenText.

Com quem devo falar para obter informações adicionais?

Se você tiver alguma dúvida ou precisar de assistência adicional, entre em contato com a sua organização de assistência usando os dados de contato fornecidos ou consulte o **site da OpenText** para obter os dados de contato em todo o mundo.

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

AMÉRICA DO NORTE +800 499 6544 • ESTADOS UNIDOS +1 847 267 9330 • ALEMANHA +49 89 4629 0

REINO UNIDO +44 0 1189 848 000 • AUSTRÁLIA +61 2 9026 3400