OPENTEXT | GXS

Comunicado de Segurança

Os gateways de comunicação da GXS podem estar vulneráveis ao bug POODLE (Padding Oracle on Downloaded Legacy Encryption).

Leia este comunicado para determinar se o seu site está vulnerável e aprender a mitigar essa vulnerabilidade.

Sistemas afetados

- Todos os gateways de comunicação que permitem aos assinantes da GXS enviar ou receber arquivos através do protocolo de comunicação SSL (Secure Sockets Layer).

Detalhes

O protocolo utilizado por gateways de comunicação da GXS para estabelecer uma conexão SSL pode estar vulnerável ao bug POODLE (CVE-2.014-3.566). Ataques do tipo POODLE são extremamente difíceis de executar e requerem que mais de 250 tentativas de transações para revelar um único byte de dados.

Impacto

Qualquer serviço que suporte SSL versão 3 (SSLv3) pode ser explorado, de modo que um atacante pode descriptografar sessões seguras potencialmente revelando senhas e outras informações privadas. A conexão estará suscetível somente se ambos remetente e receptor suportarem o SSLv3.

Nota: Se você já utiliza o Transport Layer Security (TLS) 1.0 ou posterior para acessar os gateways de comunicação da GXS, não será afetado pelo problema documentado neste Comunicado de Segurança. Entre em contato com o seu administrador de aplicativos internos ou provedor de software para garantir que está usando o TLS 1.0 ou posterior para se conectar aos nossos serviços.

Solução

A OpenText desabilitará o SSL para evitar que ele seja usado para acessar os gateways de comunicação da GXS. Em vez disso, a OpenText usará o TLS 1.0, que é um protocolo mais recente, e não é afetado pelo bug POODLE. Os planos de reparação estão sendo finalizados e serão comunicadas em breve.

Para se preparar para esta mudança e ajudar a evitar qualquer interrupção no serviço, os clientes devem atualizar proativamente o seu software de comunicação para garantir que ele suporte o TLS no modo fallback (TLS 1.2, 1.1 e 1.0).

Nota: Se você utiliza um pacote de software de terceiros para se conectar aos nossos serviços, a OpenText recomenda que entre em contato com o seu fornecedor de software o mais rápido possível para garantir que o TLS é suportado e que você pode desabilitar o SSL com segurança.

Mais informações

Para obter mais informações, consulte a FAQ ou entre em contato com o Suporte ao Cliente da GXS.

www.gxs.com.br
www.opentext.com.br