OPENTEXT™ | GXS™

安全报告

GXS 通信网关可能易受 POODLE（Padding Oracle on Downloaded Legacy Encryption，降级传统加密填充提示）漏洞的攻击。

请阅读本报告以确定您的网站是否易受攻击，并了解如果控制这种漏洞。

受到影响的系统

- 通过安全套接层（SSL）通信协议让订户能够发送或接收文件的所有 GXS 通信网关。

细节

GXS 通信网关用于建立 SSL 连接的协议可能易受 POODLE 漏洞(CVE-2014-3566)的攻击。POODLE 攻击非常难以实施，且要求超过 250 次交易尝试才能泄漏单个字节的数据。

影响

支持 SSL 第 3 版（SSLv3）的任何服务都会被利用，使得攻击者能解密安全会话，有可能泄露密码和其他隐私信息。只有当发送方和接收方均支持 SSLv3 时，该连接才会易受攻击。

注：如果您已经使用传输层安全（TLS）1.0 或其后版本访问 GXS 通信网关，您不会受此安全报告中记录的问题影响。请联系您的内部应用程序管理员或软件供应商以确保您正在使用 TLS 1.0 或其后版本连至我们的服务。

解决方案

OpenText 将停用 SSL，以防止其被用于访问 GXS 通信网关。OpenText 将代之以 TLS 1.0，这是不受 POODLE 漏洞影响的更新协议。矫正计划正在完成中，将很快宣布该计划。

为了准备这一改变，并帮助防止服务出现任何混乱，客户应主动更新各自的通信软件，以确保其在后备模式中支持 TLS（TLS 1.2、1.1 和 1.0）。

注：如果您使用第三方软件连至我们的服务，OpenText 建议您尽快联系您的软件供应商，以确保其支持 TLS，且您能安全地停用 SSL。

更多信息

如欲了解更多信息，请参阅“常见问题”或联系 GXS 客户支持。