OPENTEXT™

POODLE 漏洞

常见问题解答

如何使用本文件？

此“常见问题解答”回答了客户针对 POODLE 漏洞最常提出的一些问题。这是一份动态文件，将在 http://techsupport.gxs.com/ 定期更新。

什么是 POODLE？

POODLE 的全称是 **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption（降级传统加密填充提示）。正如其名称所示，此安全问题乃是一种协议降级，给人以利用过时加密形式的可乘之机。当谷歌发表了题为《这条狗会咬人：利用 SSL 3.0 回退模式 (This POODLE Bites:Exploiting The SSL 3.0 Fallback)》的文章后，这一问题引起了全世界的注意。

POODLE 如何工作？

攻击者借助 POODLE 发起*中间人攻击*，强迫连接“回退”至 SSLv 3（安全套接字层 3.0 版），试图获取敏感的用户数据。可能泄露的数据取决于所启用的 SSL 连接类型。

此漏洞被评级为中等。这意味着，此漏洞给了攻击者可乘之机，借此损害数据元素机密性、完整性和/或可用性，但漏洞攻击还需要一项或多项其他前提条件。POODLE 攻击非常难以实施，且 250 次以上事务尝试才能发现单个字节的数据。

OpenText 正在采取哪些措施来保护客户？

OpenText 的安全专家目前正在分析有关 POODLE 的风险。必要时，OpenText 将禁用 SSL 3 及更早版本，以防止其被用于访问 GXS 通信网关。相反，OpenText 将使用传输层安全协议 (TLS)，这是能够有效抵御 POODLE 攻击的推荐协议版本。

我会受到怎样的影响？

任何支持安全套接字层 (SSL) 第 3 版 (SSLv3) 的服务都可能被攻击者用来解密安全会话，因此可能会泄露用户数据。

只有当发送方和接收方均支持 SSLv3 时，该连接才会容易遭到 POODLE 攻击。如果已经禁用 SSLv3，您不会受上述问题的影响。OpenText 建议联系您的内部应用程序管理员或软件供应商，以确保正在使用 TLS 1.0 或更高版本（在禁用 SSLv3 的前提下）连至我们的服务。

我需要做什么？

OpenText 将分阶段更新通信网关上受影响的协议。补救计划正在制定中，更新日期的细节会很快发布。如果计划的更新日期前有任何变动，我们会向客户发出合理通知。

同时，客户应主动确保其通信软件支持 TLS 的回退模式（TLS 1.2、1.1 和 1.0）。如果使用情况允许，OpenText 建议您立刻禁用 SSL。如对 SSL 禁用方法有任何问题，请联系您的软件供应商。

哪些浏览器受 POODLE 影响？

对于基于浏览器的应用程序，所有使用 SSLv3 的网络浏览器都有风险。尽管大多数现代网页浏览器（Chrome、Firefox、Safari 和 Internet Explorer 9+）都使用 TLS 1.0 或更高版本，但 Internet Explorer 6 等旧浏览器仅支持 SSLv3。这意味着，还在使用较老版本电脑和浏览器的用户可能受 POODLE 漏洞的影响。

如果不更新浏览器，而想访问 OpenText 的服务，我的账户会出现什么情况？

尽管您的账户不会被关闭，但此种连接将被拒绝，而您将无法访问 OpenText 的服务。

哪些连接方法易受 POODLE 攻击？

OpenText 信息安全部门正在进行分析，以确定 POODLE 对用于连接至 OpenText 服务的各种通信协议造成的风险。使用 SSL 安全功能的通信协议如下所列：

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

如果您或您的贸易伙伴使用上述任一通信协议，现在也不用太担心。OpenText 正在对各协议进行风险分析，以确定哪些协议要求禁用 SSL。我们将在计划的更新日期前（正常为 60 天），向受影响客户提供有关变化的合理通知。

如何禁用 SSLv3？

浏览器：
互联网上有很多资源提供有关禁用浏览器中 SSLv3 支持的说明。其中一个例子是：
https://zmap.io/sslv3/browsers.html。

连接软件：
如果使用第三方软件包连接我们的服务，OpenText 建议您尽快联系软件提供商，确保软件支持 TLS 且 SSL 可被安全禁用。

如何知道我的服务是否受到补救计划影响？

每个通信协议的客户建议函中均列出了使用 SSL 安全功能且会受补救计划影响的 网关 URL。要查看这些网关 URL，请访问我们的网站下载与您的通信协议对应的建议函。

何时将关闭与我的通信协议对应的 SSL？

OpenText 将分阶段更新通信网关上受影响的协议。补救计划正在制定中，更新日期的细节会很快发布。要查看已完成补救的通信协议明细，请访问我们的网站。

我的系统无法支持传输层安全协议 (TLS)。该怎么办？

虽然 OpenText 将禁用 SSL 推荐为应对 POODLE 威胁的最有效方式，但是，我们知道并非所有客户都支持传输层安全协议 (TLS)。如果您的系统不支持 TLS，可借助 OpenText GXS 已经建立的例外列表，继续使用 SSL 访问 GXS 网络。要继续使用 SSL，您应访问我们的网站，将您的公司添加到我们的例外列表中。

我的贸易合作伙伴该怎么办？

随着通信网关完成补救，客户和贸易合作伙伴将需要使用 TLS 与 OpenText GXS 通信网关建立消息交换连接。客户应负责通知其贸易合作伙伴采取必要操作，应对即将到来的 POODLE 补救。

如果您的贸易合作伙伴直接连接 OpenText 服务，但不支持传输层安全协议 (TLS) 且希望被添加到例外列表，则他们需要向 OpenText 提供自己的 IP 地址。

如果需要更多信息，应与谁联系？

如有任何问题或需要更多帮助，您可联系自己的支持机构，或者访问 **OpenText 网站**，查找全球联系信息。

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

北美 +800 499 6544 • 美国 +1 847 267 9330 • 德国 +49 89 4629 0

英国 +44 0 1189 848 000 • 澳大利亚 +61 2 9026 3400