OPENTEXT™

# POODLE 漏洞

常見問題

# 如何使用本文件？

本常見問題解答了客戶針對 POODLE 漏洞最常提出的一些疑問。這是一份定期更新的文件，可到 http://techsupport.gxs.com/ 閱覽。

# 什麼是 POODLE？

POODLE 是 **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption 的縮寫。此安全問題正如其名稱所示，是指因協定降級而使過時的加密格式遭到利用。Google 發表的一份報告《 This POODLE Bites:Exploiting The SSL 3.0 Fallback》讓這個問題受到全球關注。

# POODLE 如何運作？

POODLE 可讓攻擊者執行*中間人*攻擊，也就是強制連線「退而使用」安全通訊端層 (SSL) 3.0 版，這樣攻擊者就有可能取得敏感的使用者資料。視啟用的 SSL 連線類型而定，有暴露風險的資料可能有所不同。

這個漏洞的嚴重等級是中等。這表示該問題讓攻擊者有機會危及資料元素的機密性、完整性及/或可用性，但必須存在一或多個先決條件才能成功。POODLE 攻擊極難執行；需要超過 250 次的交易嘗試才能洩漏一個位元組的資料。

# OpenText 採取哪些措施來保護客戶？

OpenText 的安全專家正在分析 POODLE 的相關風險。若有必要，OpenText 將停用 SSL 第 3 版及更舊版本，以避免被用來存取 GXS 通訊閘道。OpenText 將改用傳輸層安全協定 (TLS)，也就是建議用來抵禦 POODLE 攻擊的協定版本。

# 對我有什麼影響？

所有支援安全通訊端層 (SSL) 第 3 版 (SSLv3) 的服務都可能會遭到利用，讓攻擊者能夠解密安全的工作階段，進而洩漏使用者資料。

只有在傳送者與接收者都支援 SSLv3 的情況下，連線才有可能受到 POODLE 攻擊影響。如果您已停用 SSLv3，就不會受上述問題影響。OpenText 建議您與您的內部應用程式管理員或軟體供應商聯絡，確保使用 TLS 1.0 或更新版本 (且已停用 SSLv3) 來連接至我們的服務。

# 我必須採取哪些措施？

OpenText 會分段更新受影響的通訊閘道上的協定。補救方案尚未定案，我們稍後會通告有關轉移日期的細節。客戶會在預定的轉移日期前，經適當方式收到變更通知。

在這段期間，客戶應主動確保其通訊軟體能以後備模式支援 TLS (TLS 1.2、1.1 及 1.0)。在您的使用案例容許的情況下，OpenText 建議您立即停用 SSL。如果對於如何停用 SSL 有任何疑問，請聯絡您的軟體供應商。

## 哪些瀏覽器會受到 POODLE 影響？

就瀏覽器型應用程式而言，所有使用 SSLv3 的網頁瀏覽器都會受到影響。雖然絕大多數的現代網頁瀏覽器 (Chrome、Firefox、Safari 及 Internet Explorer 9+) 都使用 TLS 1.0 或更新版本，但舊式瀏覽器 (例如 Internet Explorer 6) 只支援 SSLv3。換言之，使用舊型電腦及舊版瀏覽器版本的使用者，都有可能受到 POODLE 漏洞的影響。

## 如果我沒有更新瀏覽器而嘗試使用 OpenText 服務，我的帳戶會怎樣？

雖然您的帳戶不會被關閉，但連線會遭拒，而您將無法使用 OpenText 服務。

## 哪些連線方式會受到 POODLE 影響？

OpenText 資訊安全部門正在進行分析，判斷 POODLE 對於用來連接至 OpenText 服務的各種通訊協定有哪些風險。使用 SSL 安全功能的通訊協定如下：

- HTTP
- FTP
- AS2
- RosettaNet
- OFTP
- MQ
- AS3

假使您或您的貿易合作夥伴使用上述任何一種通訊協定，也毋需立即擔憂。OpenText 正在對每種協定進行風險分析，判斷要停用哪些需要 SSL 的協定。受影響的客戶會在預定的轉移日期 (通常是 60 日) 前，經適當方式收到變更通知。

## 如何停用 SSLv3？

瀏覽器：
網路上有許多資源，可教導您如何停用瀏覽器中的 SSLv3 支援。其中一例是 https://zmap.io/sslv3/browsers.html。

連線軟體：

如果您使用第三方軟體套件連接至我們的服務，那麼 OpenText 建議您儘快聯絡您的軟體供應商以確保相關軟體可支援 TLS，讓您能夠安全地停用 SSL。

## 我如何知道我的服務是否在補救方案的範圍內？

每份通訊協定的客戶報告都會包含使用 SSL 安全功能且在補救方案範圍內的閘道 URL 列表。若要檢閱閘道 URL 列表，請造訪我們的網站並下載您通訊協定的報告。

## 我的通訊閘道何時會關閉 SSL？

OpenText 會分段更新受影響的通訊閘道上的協定。補救方案尚未定案，我們稍後會通告有關轉移日期的細節。若要檢閱已補救之通訊協定的時間表，請造訪我們的網站。

## 我的系統無法支援傳輸層安全協定 (TLS)。我該怎麼辦？

雖然 OpenText 建議，應對 POODLE 威脅最有效的方式就是停用 SSL，但是我們知道，並非所有客戶都能夠支援傳輸層安全協定 (TLS)。如果您無法支援 TLS，那麼 OpenText GXS 建立的特殊情況列表可讓客戶透過 SSL 繼續使用 GXS 網路。您必須造訪我們的網站，將貴公司添加到我們的特殊情況列表，才能繼續使用 SSL。

## 我的貿易合作夥伴該怎麼辦？

補救通訊閘道之後，客戶與貿易合作夥伴必須使用 TLS 建立透過 OpenText GXS 通訊閘道進行的訊息交換連線。客戶應負責告知其貿易合作夥伴有關必須採取的動作，以便為日後的 POODLE 補救方案做好準備。

如果您的貿易合作夥伴是直接連接至 OpenText 服務且無法支援傳輸層安全協定 (TLS)，但希望被添加到特殊情況列表，則必須將其 IP 位址提供給 OpenText。

## 我應該向誰索取進一步資料？

如果您有任何疑問或需要更多協助，可以根據提供給您的聯絡資料向您的支援組織洽詢，或是造訪 **OpenText 網站** 查閱全球聯絡資料。

# 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**

北美洲 +800 499 6544 • 美國 +1 847 267 9330 • 德國 +49 89 4629 0

英國 +44 0 1189 848 000 • 澳洲 +61 2 9026 3400

Copyright ©2013-2014 Open Text Corporation
OpenText 是 Open Text SA 及/或 Open Text ULC 的商標或註冊商標。商標列表所提及 (但不限於) 之其他商標、註冊商標、產品名稱、公司名稱、品牌及服務名稱皆為 Open Text SA 或其他個別擁有者的財產。保留一切權利。如需更多資訊，請造訪 http://www.opentext.com/2/global/site-copyright.html SKU#