OPENTEXT™ | GXS™

安全通報

GXS 通訊閘道可能受 Padding Oracle on Downloaded Legacy Encryption (POODLE) 錯誤影響。

請參閱本通報，判斷您的網站是否受影響，並了解如何減低影響。

受影響系統

- 所有讓用戶透過安全通訊端層 (SSL) 通訊協定收發檔案的 GXS 通訊閘道。

詳情

GXS 通訊閘道用來建立 SSL 連接的協定，可能受 POODLE 錯誤影響 (CVE-2014-3566)。POODLE 攻擊極難執行，必須作出超過 250 項交易嘗試才能顯露一個位元組 (byte) 的數據。

影響

任何支援 SSL 版本 3 (SSLv3) 的服務都可能受影響，讓攻擊者能將安全工作階段 (secure session) 解密，也許會暴露密碼及其他私人資料。只有在傳送者與接收者都支援 SSLv3 的情況下，網絡連接才可能受到影響。

請注意：如果您已透過傳輸層安全協定 (TLS) 1.0 或較新版本使用 GXS 的通訊閘道，就不受本安全通報所述的問題影響。請聯絡您的內部程式管理員或軟體供應商，確保您正在透過 TLS 1.0 或較新版本連接我們的服務。

解決辦法

OpenText 會停用 SSL 以防被利用進入 GXS 通訊閘道，並改用較新及不受 POODLE 錯誤 (bug) 影響的 TLS 1.0。補救方案即將定案，稍後會有宣布。

為準備應付上述變更，及協助防止任何服務中斷，客戶應積極更新通訊軟體，確保能支援 TLS (TLS 1.2、1.1 及 1.0) 作為後備模式。

請注意：假如您以第三方軟體套件連接我們的服務，OpenText 建議您盡早聯絡您的軟體供應商，確保有關軟體能支援 TLS，讓您可以安全停用 SSL。

詳細資訊

欲知詳情，請參閱常見問題，或聯絡 GXS 客戶支援。