OPENTEXT | GXS

Sicherheitsempfehlung

GXS-Kommunikationsgateways können für den POODLE-Bug (Oracle on Downloaded Legacy Encryption) anfällig sein.

Lesen Sie diese Sicherheitsempfehlung, um zu ermitteln, ob Ihre Website gefährdet ist, und um zu erfahren, wie diese Sicherheitsanfälligkeit behoben werden kann.

Betroffene Systeme

- Alle GXS-Kommunikationsgateways, die es Nutzern ermöglichen, unter Verwendung des SSL (Secure Sockets Layer)-Kommunikationsprotokolls Dateien zu senden oder zu empfangen.

Details

Das Protokoll, das von GXS-Communikationgateways zum Herstellen einer SSL-Verbindung verwendet wird, ist möglicherweise für den POODLE-Bug (CVE-2014-3566) anfällig. POODLE-Angriffe sind äußerst schwierig auszuführen und zur Offenlegung eines Datenbytes sind mehr als 250 Transaktionsversuche erforderlich.

Auswirkungen

Jeder Dienst, der SSL Version 3 (SSLv3) unterstützt, kann ausgenutzt werden, sodass ein Angreifer sichere Sitzungen entschlüsseln und potenziell Kennwörter und andere vertrauliche Informationen offenlegen kann. Eine Verbindung ist nur dann anfällig, wenn Absender und Empfänger SSLv3 unterstützen.

Hinweis: Wenn Sie bereits TLS (Transport Layer Security) 1.0 oder höher für den Zugriff auf GXS-Kommunikationsgateways verwenden, sind Sie von dem in dieser Sicherheitsempfehlung dokumentierten Problem nicht betroffen. Kontaktieren Sie Ihren internen Anwendungsadministrator oder den Softwareanbieter, um sicherzustellen, dass Sie TLS 1.0 oder höher für die Verbindung mit unseren Diensten verwenden.

Lösung

OpenText deaktiviert SSL, um zu verhindern, dass dieses Protokoll für den Zugriff auf GXS-Kommunikationsgateways verwendet wird. Stattdessen verwendet OpenText TLS 1.0, ein neueres Protokoll, das vom POODLE-Bug nicht betroffen ist. Die Problembehebungspläne werden gerade fertig gestellt und werden in Kürze bekannt gegeben.

Um sich auf diese Änderung vorzubereiten und Dienstunterbrechungen zu verhindern, sollten die Kunden vorsorglich ihre Kommunikationssoftware aktualisieren, um sicherzustellen, dass die Software TLS im Fallbackmodus unterstützt (TLS 1.2, 1.1 und 1.0).

Hinweis: Wenn Sie über ein Softwarepaket eines Fremdherstellers auf unsere Dienste zugreifen, empfiehlt OpenText Ihnen, den Softwareanbieter sobald wie möglich zu kontaktieren, um sicherzustellen, dass TLS unterstützt wird und Sie SSL gefahrlos deaktivieren können.

Weitere Informationen

Weitere Informationen finden Sie in den häufig gestellten Fragen (FAQ) oder erhalten Sie vom GXS Customer Support.