OPENTEXT™

POODLE-Sicherheitsanfälligkeit

Häufig gestellte Fragen

Wie verwende ich dieses Dokument?

Dieses Dokument (FAQ) enthält Antworten zu einigen der Fragen, die von unseren Kunden am häufigsten zur POODLE-Sicherheitslücke gestellt werden. Dies ist ein laufend fortzuschreibendes Dokument, das regelmäßig auf der Website http://techsupport.gxs.com/ aktualisiert wird.

Was ist POODLE?

POODLE ist ein Akronym für **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption. Wie der Name nahelegt, besteht das Sicherheitsproblem in einer Protokollherabstufung, die es ermöglicht, ein veraltetes Verschlüsselungsformat für Angriffe auszunutzen. Öffentlich bekannt wurde das Problem durch eine Veröffentlichung von Google mit dem Titel This POODLE Bites: Exploiting The SSL 3.0 Fallback.

Wie funktioniert POODLE?

POODLE ermöglicht einem Angreifer einen *Man-in-the-Middle*-Angriff, der eine Verbindung u. U. dazu zwingen kann, auf Secure Sockets Layer (SSL) Version 3.0 auszuweichen (engl. fallback), und es dem Angreifer dadurch ermöglicht, in den Besitz von vertraulichen Benutzerdaten zu gelangen. Bei welchen Daten ein Risiko der Offenlegung besteht, ist vom Typ der aktivierten SSL-Konnektivität abhängig.

Diese Sicherheitsanfälligkeit wurde als Mittel eingestuft. Das bedeutet, dass dieses Problem Angreifern die Möglichkeit bietet, die Vertraulichkeit, Integrität und/oder Verfügbarkeit von Datenelementen zu gefährden, wobei allerdings mindestens eine Vorbedingung erfüllt sein muss. Ein POODLE-Angriff ist schwierig auszuführen und zur Offenlegung eines Datenbytes sind mehr als 250 Transaktionsversuche erforderlich.

Was unternimmt OpenText, um die Kunden zu schützen?

Sicherheitsexperten von OpenText analysieren derzeit die mit POODLE verbundenen Risiken. Falls erforderlich, deaktiviert OpenText das Protokoll SSL Version 3 oder älter, um zu verhindern, dass es für den Zugriff auf GXS-Kommunikationsgateways verwendet wird. Stattdessen wird OpenText künftig das zum Schutz gegen POODLE-Angriffe empfohlene Protokoll TLS 1.0 verwenden.

Inwiefern bin ich davon betroffen?

Jeder Dienst, der Secure Sockets Layer (SSL) Version 3 (SSLv3) unterstützt, kann ausgenutzt werden, sodass ein Angreifer sichere Sitzungen entschlüsseln und potenziell Benutzerdaten offenlegen kann.

Eine Verbindung ist nur dann anfällig für einen POODLE-Angriff, wenn sowohl Absender als auch Empfänger SSLv3 unterstützen. Wenn Sie SSLv3 bereits deaktiviert haben, sind Sie von dem oben beschriebenen Problem nicht betroffen. OpenText empfiehlt Ihnen, Ihren internen Anwendungsadministrator oder den Softwareanbieter zu kontaktieren, um sicherzustellen, dass Sie TLS 1.0 oder höher für die Verbindung mit unseren Diensten verwenden.

Was muss ich tun?

OpenText aktualisiert das Protokoll der betroffenen Kommunikationsgateways stufenweise. Die Problembehebungspläne werden gerade fertig gestellt und nähere Angaben zu den Umstellungsterminen werden in Kürze mitgeteilt. Die Kunden werden in angemessener Frist vor den geplanten Umstellungsterminen auf die Änderungen hingewiesen.

Zwischenzeitlich sollten die Kunden vorsorglich sicherstellen, dass ihre Kommunikationssoftware TLS im Fallbackmodus unterstützt (TLS 1.2, 1.1 und 1.0). Wenn Ihre Anwendung dies erlaubt, empfiehlt OpenText, SSL sofort zu deaktivieren. Bitte wenden Sie sich an den Softwareanbieter, wenn Sie Fragen zur Deaktivierung von SSL haben.

Welche Browser sind von POODLE betroffen?

Bei browserbasierten Anwendungen ist jeder Browser, der SSLv3 verwendet, gefährdet. Der Großteil der modernen Webbrowser (Chrome, Firefox, Safari und Internet Explorer 9+) verwendet zwar TLS 1.0 und höher, aber ältere Browser, z. B. Internet Explorer 6, unterstützen nur SSLv3. Das bedeutet, dass Benutzer, die ältere PCs oder Browserversionen verwenden, möglicherweise von der POODLE-Sicherheitsanfälligkeit betroffen sind.

Was geschieht mit meinem Konto, wenn ich auf OpenText-Dienste zuzugreifen versuche, ohne meinen Browser aktualisiert zu haben?

Ihr Konto wird zwar nicht deaktiviert, aber die Verbindung wird abgelehnt, und daher können Sie nicht auf die OpenText-Dienste zugreifen.

Welche Verbindungsmethoden können für POODLE anfällig sein?

OpenText Information Security analysiert derzeit, welches Risiko POODLE für die verschiedenen Kommunikationsprotokolle darstellt, die für den Verbindungsaufbau mit OpenText-Diensten verwendet werden. Folgende Kommunikationsprotokolle nutzen die Sicherheitsfunktionen von SSL:

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

Wenn Sie oder Ihr(e) Handelspartner eines der oben aufgeführten Kommunikationsprotokolle verwenden, besteht kein unmittelbarer Grund zur Sorge. OpenText erstellt für jedes Protokoll eine Risikoanalyse, um zu bestimmen, bei welchen Protokollen SSL deaktiviert werden muss. Die betroffenen Kunden werden in angemessener Frist vor den geplanten Umstellungsterminen (normalerweise 60 Tage) auf die Änderungen hingewiesen.

Wie deaktiviere ich SSLv3?

Browser:
Im Internet sind viele Ressourcen verfügbar, die Anleitungen zum Deaktivieren der SSLv3-Unterstützung in Browsern enthalten. Ein Beispiel hierfür ist https://zmap.io/sslv3/browsers.html.

Verbindungssoftware:
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.

Wie kann ich feststellen, ob meine Dienste von dem POODLE-Abwehrplan betroffen sind?

In den Kundenhinweisen zu jedem Kommunikationsprotokoll sind die Gateway-URLs aufgeführt, die Sicherheitsfunktionen von SSL nutzen und daher von dem POODLE-Abwehrplan betroffen sind. Bitte laden Sie den Hinweis für Ihr Kommunikationsprotokoll von unserer Webseite herunter, um die Liste der Gateway-URLs zu prüfen.

Wann wird SSL für mein Kommunikationsgateway abgeschaltet?

OpenText aktualisiert das Protokoll der betroffenen Kommunikationsgateways stufenweise. Die Abwehrpläne werden gerade fertig gestellt und nähere Angaben zu den Umstellungsterminen werden in Kürze mitgeteilt. Die Zeitpläne für bereits aktualisierte Kommunikationsprotokolle finden Sie auf unserer Webseite.

Mein System bietet keine Möglichkeit zur Nutzung der Transport Layer Security (TLS). Was soll ich tun?

OpenText empfiehlt zwar die Deaktivierung von SSL als effektivstes Verfahren zum Schutz gegen POODLE-Angriffe, ist sich jedoch der Tatsache bewusst, dass nicht alle Kunden TLS (Transport Layer Security) nutzen können. Sollten Sie keine Möglichkeit zur Nutzung von TLS haben, können Sie sich in eine Ausnahmeliste von OpenText GXS eintragen, so dass Sie weiterhin mit SSL-Verschlüsselung auf das GXS-Netzwerk zugreifen können. Um weiterhin SSL nutzen zu können, müssen Sie Ihr Unternehmen auf unserer Website in die Ausnahmeliste eintragen.

Was geschieht mit meinen Handelspartnern?

Nach der Aktualisierung der Kommunikationsgateways müssen Kunden und Handelspartner Nachrichtenaustauschverbindungen mit OpenText GXS-Kommunikationsgateways über TLS herstellen. Es ist Aufgabe jedes Kunden, seine Handelspartner über die erforderlichen Maßnahmen zur Vorbereitung der bevorstehenden Umstellung zwecks POODLE-Abwehr zu informieren.

Sollten Sie einen Handelspartner haben, der direkte Verbindungen mit OpenText-Diensten herstellt, jedoch keine Möglichkeit zur Nutzung der Transport Layer Security (TLS) hat und deshalb in die Ausnahmeliste aufgenommen werden möchte, muss dieser seine IP-Adresse an OpenText übermitteln.

An wen kann ich mich wenden, um weitere Informationen zu erhalten?

Wenn Sie Fragen haben oder weitere Unterstützung benötigen, können Sie sich unter Verwendung der Kontaktdaten, die Ihnen mitgeteilt wurden, an die für Sie zuständige Supportniederlassung wenden, oder Sie besuchen die **OpenText-Website** wo Sie weltweite Kontaktinformationen finden.

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

NORDAMERIKA +800 499 6544 • USA +1 847 267 9330 • DEUTSCHLAND 89 4629 4629-0

GROSSBRITANNIEN +44 0 1189 848 000 • AUSTRALIEN +61 2 9026 3400