OPENTEXT™

POODLE 취약점

자주 묻는 질문

이 문서의 용도는 무엇입니까?

이 FAQ 에서는 고객이 POODLE 취약점과 관련하여 자주 묻는 일부 질문들에 대한 답변을 제시하고 있습니다. 이 문서는 정기적으로 업데이트되며 http://techsupport.gxs.com/을 참조하십시오.

POODLE 이란 무엇입니까?

POODLE 은 **P**adding **O**racle **O**n **D**owngraded **L**egacy **E**ncryption(다운그레이드된 구식 암호화에 대한 패딩 오라클)의 약자입니다. 이와 관련한 보안 문제는 이름이 뜻하는 바와 같이 구식 암호화 기법을 악용할 수 있게 하는 프로토콜 다운그레이드입니다. 이 문제는 구글이 This POODLE Bites: Exploiting The SSL 3.0 Fallback 이라는 논문을 발표하면서 세간의 주목을 받게 됐습니다.

POODLE 공격은 어떻게 수행됩니까?

POODLE 을 이용하는 공격자는 SSL(Secure Sockets Layer) 버전 3.0 에 강제 "폴백"(fallback) 연결할 수 있는 중간자 공격(man-in-the-middle attack)을 수행하여 민감한 사용자 데이터를 탈취할 수 있습니다. 노출 위험이 있는 데이터는 활성화된 SSL 연결의 종류에 따라 다를 수 있습니다.

이 취약점은 중간 등급입니다. 이와 같은 문제로 공격자는 데이터 요소의 기밀성, 무결성 및/또는 유효성을 위태롭게 할 기회를 갖게 되지만, 그러기 위해서는 하나 이상의 전제 조건이 필요합니다. POODLE 공격은 실행이 상당히 어려우며 단 1 바이트의 데이터를 표시하는 데에도 250 번 이상의 트랜잭션을 시도해야 합니다.

OpenText 의 고객 보호 대책은 무엇입니까?

OpenText 의 보안 전문가들은 현재 POODLE 과 관련한 위험을 분석하고 있습니다. 필요한 경우, OpenText 는 SSL 3 이전 버전을 비활성화하여 GXS 통신 게이트웨이에 액세스하지 못하게 할 것입니다. 대신, POODLE 공격으로부터 보호하는 권장 프로토콜 버전인 TLS(Transport Layer Security)를 사용하게 됩니다.

사용자에게 미치는 영향은 무엇입니까?

SSL 버전 3(SSLv3)을 지원하는 모든 서비스는 악용될 우려가 있으며 공격자가 보안 세션을 해독하여 잠재적으로 사용자 데이터가 드러날 수 있습니다.

송신자와 수신자가 모두 SSLv3 를 지원하는 상태에서 연결하는 경우에만 POODLE 공격에 취약합니다. SSLv3 를 이미 비활성화시켰다면 위에서 설명한 문제의 영향을 받지 않습니다.

OpenText 는 내부 애플리케이션 관리자 또는 소프트웨어 제공 업체에 연락하여 OpenText 서비스 연결을 위해 SSLv3 이 비활성화된 TLS 1.0 이상 버전을 사용하고 있는지 확인할 것을 권장합니다.

사용자가 해야 할 일은 무엇입니까?

OpenText 는 각 단계에서 영향을 받은 통신 게이트웨이의 프로토콜을 업데이트합니다. 개선 계획이 마무리되는 대로 롤오버 날짜에 관한 상세 내용을 곧 알려드릴 예정입니다. 변경 내용은 계획된 롤오버 날짜 전에 고객에게 사전 고지될 것입니다.

고객은 통신 소프트웨어가 폴백 모드에서 TLS 를 지원하도록 사전 업데이트하셔야 합니다(TLS 1.2, 1.1 및 1.0). 가능한 경우, SSL 을 즉시 비활성화하실 것을 권장합니다. SSL 비활성화 방법에 대해 궁금한 사항은 소프트웨어 제공 업체에 문의하십시오.

POODLE 에 영향을 받는 브라우저는 무엇입니까?

브라우저 기반 애플리케이션의 경우, SSLv3 을 사용하는 모든 웹 브라우저가 위험합니다. 대다수의 최신 웹 브라우저(크롬, 파이어폭스, 사파리, Internet Explorer 9 이상)가 TLS 1.0 이상 버전을 사용하고 있다 해도 Internet Explorer 6 같은 구형 브라우저는 SSLv3 만 지원합니다. 이는 구형 PC 와 브라우저를 쓰는 사용자들은 POODLE 취약점의 영향을 받을 수 있다는 뜻입니다.

업데이트하지 않은 브라우저로 OpenText 서비스를 이용하려 하는 경우 사용자 계정에 미치는 영향은 무엇입니까?

계정이 폐쇄되지는 않아도 연결이 거부되어 OpenText 서비스를 이용할 수 없게 됩니다.

POODLE 에 취약할 수 있는 연결 방식은 무엇입니까?

OpenText Information Security 는 POODLE 이 OpenText 서비스에 연결하기 위해 사용되는 다양한 통신 프로토콜에 초래하는 위험을 판별하기 위하여 분석을 수행하고 있습니다. SSL 의 보안 기능을 사용하는 통신 프로토콜은 다음과 같습니다.

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

사용자 또는 사용자의 상대 파트너가 상기 통신 프로토콜 중 어느 것이든 사용하고 있다면 당장 우려할 만한 위험은 없습니다. OpenText 는 SSL 을 비활성화해야 하는 프로토콜을 판명하기 위해 각 프로토콜에 대한 위험 분석을 수행하고 있습니다. 변경 내용은 계획된 롤오버 날짜 전에(대개 60 일 전) 영향을 받는 고객에게 사전 고지될 것입니다.

SSLv3 비활성화하려면 어떻게 해야 합니까?

브라우저:
인터넷을 통해 브라우저에서 SSLv3 를 비활성화하는 방법에 대한 다양한 정보를 확인할 수 있습니다. 예: https://zmap.io/sslv3/browsers.html

연결 소프트웨어:
사용자가 제삼자 소프트웨어 패키지로 OpenText 서비스에 연결하는 경우, 소프트웨어 제공 업체에 가능한 한 빨리 연락하여 TLS 이 지원되는지 확인하고 SSL 을 안전하게 비활성화하시기 바랍니다.

내 RosettaNet 서비스가 리미디에이션 계획에 영향을 받는지 어떻게 알 수 있습니까?

각 통신 프로토콜에 대한 고객 주의보는 SSL 의 보안 기능을 사용하고 리미디에이션 계획의 영향을 받는 게이트웨이 URL 목록을 포함합니다. 게이트웨이 URL 목록을 확인하려면 OpenText 웹사이트를 방문하여 통신 프로토콜에 대한 주의보를 다운로드받으십시오.

언제 내 통신 게이트웨이에 대해 SSL 이 비활성화됩니까?

OpenText 는 각 단계에서 영향을 받은 통신 게이트웨이의 프로토콜을 업데이트합니다. 개선 계획이 마무리되는 대로 롤오버 날짜에 관한 상세 내용을 곧 알려드릴 예정입니다. 이미 업데이트 관리된 통신 프로토콜에 대한 일정을 확인하려면 OpenText 웹사이트를 참조하십시오.

내 시스템은 TLS (Transport Layer Security)를 지원할 수 없습니다. 어떻게 해야 합니까?

OpenText 는 POODLE 위협을 처리하는 가장 효과적인 방법으로 SSL 비활성화를 권장하지만, 모든 고객이 TLS(Transport Layer Security)를 지원할 수 있는 것이 아니라는 것을 알고 있습니다. TLS 를 지원할 수 없는 경우, OpenText GXS 는 고객이 SSL 을 사용하여 GXS 네트워크에 계속 액세스할 수 있도록 하는 예외 목록을 설정하였습니다. SSL 을 계속해서 사용하려면 OpenText 웹사이트를 방문하여 예외 목록에 귀사를 추가해야 합니다.

내 RosettaNet 상대 파트너는 어떻게 됩니까?

통신 게이트웨이가 개선됨에 따라 고객 및 상대 파트너는 TLS 를 사용하여 OpenText GXS 통신 게이트웨이와 메시지 교환 연결을 설정해야 합니다. 고객은 상대 파트너에게 곧 수행될 POODLE 리미디에이션을 위해 준비해야 하는 모든 필요한 조치에 대해 통지할 책임이 있습니다.

상대 파트너가 OpenText 서비스에 직접 연결되어 있고 TLS(Transport Layer Security)를 지원할 수 없으며 예외 목록에 추가되기를 원하는 경우, IP 주소와 함께 OpenText 를 제공해야 합니다.

더 자세한 정보를 알고 싶으면 어떻게 해야 합니까?

궁금한 사항이나 도움이 더 필요하시면 제공된 연락처로 지원 기관에 연락하시거나 **OpenText 웹사이트** 를 방문하여 전 세계 OpenText 사무소 정보를 확인하시기 바랍니다.

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

북미 +800 499 6544 • 미국 +1 847 267 9330 • 독일 +49 89 4629 0

영국 +44 0 1189 848 000 • 호주 +61 2 9026 3400