보안 경고

GXS 통신 게이트웨이는 POODLE(Padding Oracle on Downloaded Legacy Encryption) 버그에 취약할 수 있습니다.

이 경고문을 검토하여 귀 사이트가 취약한 공격 대상인지 확인하시고 이 취약성을 보완하는 방법을 알아보시기 바랍니다.

영향을 받는 시스템

- 가입자가 Secure Sockets Layer(SSL) 통신 프로토콜로 파일을 송신 또는 수신할 수 있게 하는 모든 GXS 통신 게이트웨이

내용

GXS 통신 게이트웨이가 SSL 연결을 위하여 사용하는 프로토콜은 POODLE 버그(CVE-2014-3566)에 취약할 수 있습니다. POODLE 공격은 실행이 대단히 어려우며 250 여 트랜잭션 시도가 있어야 1 바이트의 데이터가 드러날 뿐입니다.

영향

SSL 버전 3(SSLv3)을 지원하는 모든 서비스는 악용될 수 있으므로 공격자가 보안 세션을 해독하여 잠재적으로 암호와 기타 개인 정보가 드러날 수 있습니다. 송신자와 수신자가 모두 SSLv3 를 지원하는 상태에서 연결하는 경우에만 취약합니다.

주: 이미 Transport Layer Security(TLS) 1.0 이상 버전으로 GXS 통신 게이트에 접속하고 있는 사용자는 이 보안 경고에 소개된 문제에 영향을 받지 않습니다. 내부 애플리케이션 관리자나 소프트웨어 제공 업체에 연락하여 TLS 1.0 이상 버전으로 저희 서버에 연결되게 해달라고 하십시오.

솔루션

OpenText 는 SSL 을 비활성화하여 GXS 통신 게이트웨이에 사용되지 못하게 할 것입니다. OpenText 는 그 대신 POODLE 버그에 영향을 받지 않는 가장 최근의 프로토콜인 TLS 1.0 을 사용할 것입니다. 개선 계획이 마무리되는 대로 곧 발표할 예정입니다.

이 같은 변화에 대비하고 서비스 이용에 차질이 없도록 고객은 통신 소프트웨어가 폴백 모드에서 TLS 를 지원하도록 사전 업데이트하셔야 합니다(TLS 1.2, 1.1 및 1.0).

주: 사용자가 제삼자 소프트웨어 패키지로 저희 서비스에 연결하는 경우, OpenText 는 사용자가 소프트웨어 제공 업체에 가능한 한 빨리 연락하여 TLS 이 지원되게 하고 SSL 을 안전하게 비활성화하실 것을 권합니다.

추가 정보

자세한 정보는 FAQ 를 보시거나 GXS 고객 지원부에 연락하십시오.