DROWN Notice

DROWN, which stands for "**D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption," is a man-in-the-middle attack on TLS (Transport Layer Security) that lets an attacker decrypt data on a TLS connector if the server supports SSLv2, or if the server certificate is shared with another server that supports SSLv2.

SSLv2 has been disabled by default within Jitterbit alongside our update to Apache 2.4.12 in late Spring 2015 (with the release of Jitterbit versions 8.2.0 and 5.5.2). This applies to our hosted web services only. Additionally, HTTPS has to be enabled manually on the server by the customer and the customer can choose what protocols to support.

Customers on Jitterbit versions older than 8.2.0 and 5.5.2 may be vulnerable if they have enabled hosted end points and are using HTTPS with those endpoints. Jitterbit recommends, in that situation, that the customer upgrade to the latest version of Jitterbit. If this is not possible or practical, the customer should configure their Apache server to disallow SSLv2.

Jitterbit's Cloud infrastructure does not allow SSLv2 (or SSLv3 for that matter) and is not vulnerable.

For additional information regarding DROWN, please see: https://drownattack.com/

Related Topics

- Announcements
- Hosted HTTP Endpoints
- Jitterbit Security

Last updated: May 17, 2019