DROWN Attack

by Robert Hawk

xMatters Security Office
March 1, 2016

On Tuesday, March 1, 2016, a group of independent Internet security professionals identified and announced the **D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption (DROWN) Attack, and created a website dedicated to the vulnerability [https://drownattack.com/]. The DROWN Attack exploits a protected Hyper-Text Transfer Protocol (HTTP) security mechanism such as Transport Layer Security (TLS) by using an existing vulnerability in the Secure Socket Layer (SSL) v2 code in the same library.

The xMatters cloud-based Software-as-a-Service (SaaS) does not use or enable SSL v2, and has no exposure to this vulnerability.

The DROWN Attack is a new form of cross-protocol, Bleichenbacher padding oracle attack. It allows an attacker to decrypt intercepted TLS connections by making specially crafted connections to an SSL v2 server that uses the same private key for all symmetric cipher suites. The xMatters Security Office analyzed exposure to CVE-2016-800 and found that while xMatters uses the affected code, the system configuration mitigates the vulnerability. The SSL v2 required by the vulnerability is not used by or enabled in the xMatters SaaS.

Resources:

- https://drownattack.com/
- https://www.openssl.org/news/secadv/20160301.txt
- https://drownattack.com/drown-attack-paper.pdf
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800