Entuity Software Notification

Technical Bulletin
Version 2016.03.04
March 04, 2016

DROWN Vulnerability

A major security vulnerability has been discovered in the SSLv2 protocol. The vulnerability has been referred to as DROWN (**D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption) and assigned the CVE reference CVE-2016-0800. The purpose of this notification is to explain the potential impact of this vulnerability to Entuity software and to provide references to further information on the subject.

A DROWN cross-protocol attack can decrypt TLS (Transport Layer Security) sessions by exploiting a vulnerability in the SSLv2 protocol that exposes private RSA keys.

Entuity software does not support SSLv2 so no additional Entuity patches will be required. Entuity recommends that customers refer to the following web-sites for further information and links on the subject:

DROWN Research:
https://drownattack.com

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800