MINISTRY OF
HOME AFFAIRS
CAYMAN ISLANDS GOVERNMENT

Cyber Security Awareness Bulletin:

SSLv2 DROWN Attack

03/03/2016

Original release date: March 01, 2016

Network traffic encrypted using an RSA-based SSL certificate may be decrypted if enough SSLv2 handshake data can be collected. Exploitation of this vulnerability - referred to as DROWN in public reporting - may allow a remote attacker to obtain the private key of a server supporting SSLv2.

Users and administrators are encouraged to review Vulnerability Note VU#583776 for additional mitigation details.

Source: US-CERT
