CERT-GH SECURITY ADVISORY

CERT-GH
Ghana Computer Emergency Response Team

SSLv2 DROWN Attack

CERT GH REFERENCE #: **CERT-ADV10102032016**
Severity: High
Date Discovered: 1st March 2016

System(s) Affected	SSL v2
Description	Network traffic encrypted using an RSA-based SSL certificate may be decrypted if enough SSLv2 handshake data can be collected. This is known as the "DROWN" attack in the media. Exploitation of this vulnerability may allow a remote attacker to obtain the private key of a server supporting SSLv2. "DROWN" is a new form of cross-protocol padding oracle attack. In such a case, an attacker may obtain the private key from a vulnerable server supporting SSLv2 and use it to decrypt any traffic encrypted using the shared certificate. It allows an attacker to decrypt intercepted TLS connections by making specially crafted connections to an SSLv2 server that uses the same private key. “The SSLv2 protocol is the only protocol directly impacted; however, many servers may use a shared certificate between the SSLv2 and the newer TLS protocols. If so, if the certificate is decrypted via SSLv2, then the TLS protocol using the shared certificate can be decrypted as well. The attack requires approximately 1000 SSL handshakes to be intercepted for the attack to be effective.
Impact	A remote attacker may be able to obtain the private key of a server supporting SSLv2. Servers using TLS protocol with the same shared certificate as is used for SSLv2 may also be vulnerable.
Solutions	**Disable SSLv2** Network administrators should disable SSLv2 support. The researchers have provided more information on how to disable SSLv2 for various server products. Network administrators can determine if a server supports SSLv2 with the following command: openssl s_client -connect host:443 -ssl2 If certificate information is returned, then SSLv2 is supported. SSLv2 has been deprecated since 2011.

	Do not reuse SSL certificates or key material This issue can be mitigated on TLS connections by using unique SSL keys and certificates. If possible, do not reuse key material or certificates between SSLv2 and TLS support on multiple servers. **Monitor network and use firewall rules** We recommend enabling firewall rules to block SSLv2 traffic. Since the attack requires approximately 1000 SSL handshakes, network administrators may also monitor logs to look for repeated connection attempts. However, this data may also be obtained via man-in-the-middle or other attacks, not solely from direct connections.
References & Further Information	https://www.us-cert.gov/ncas/current-activity/2016/03/01/SSLv2-DROWN-Attack https://www.us-cert.gov/ncas/current-activity/2016/03/01/OpenSSL-Releases-Security-Advisory