CyberVigilance™

A PROTEUS TECHNOLOGIES CYBER SOLUTION

#ACTB4URHACKD

RESEARCH REMEDIATE RESPOND

"It's as helpful as throwing a drowning man both ends of a rope" - Arthur Baer

DROWN stands for **D**ecrypting **R**SA with **O**bsolete and **W**eakened e**N**cryption. It allows an attacker to decrypt intercepted TLS connections by making specially crafted connections to an SSLv2 server that uses the same private key.

No Lifeguard On Duty

DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. These protocols allow everyone on the Internet to browse the web, use email, shop online, and send instant messages without third-parties being able to read the communication.

DROWN is a classic example of a cross protocol attack. This type of attack makes use of bugs in one protocol implementation (SSLv2) to attack the security of connections made under a different protocol entirely - in this case, TLS.

DROWN allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data. Current industry estimates indicate 33% of all HTTPS servers are vulnerable to the attack.

Act Before You're Hacked

If you are unsure how to protect your websites, mail servers, and other TLS-dependent services from DROWN, contact PROTEUS at CV@proteuseng.com to find out how our CyberVigilance™ services can detect and alert YOU to take the proactive measures to avoid a security breach.

PROTEUS TECHNOLOGIES
Outsmart.