Expert provides understanding of the FREAK flaw

AlienVault Senior Product Manager Andy Manoske provides an insight into this latest threat.

In light of the newly discovered ‘FREAK’ flaw that has been found to affect Google and Apple devices, Andy Manoske, senior product manager at AlienVault, has given the following comment: “Users on unpatched Android and Apple devices, as well as other embedded deviceswhich use unpatched versions of TLS/SSL, may be vulnerable to this flaw. To exploit FREAK however, such users need to connect to servers where support for downgraded export keys is still enabled and have an attacker on their network monitoring their connection with this server. “Even then this only allows attackers the opportunity to perform cryptoanalytic attacks on their ephemeral key - a key which will only be valid for their session of communication with the server. This is definitely a glaring vulnerability, but it's by no means something as dangerous or hard to remediate as Heartbleed.

“

FREAK isn't like Heartbleed or other widely-exploited vulnerabilities in 2014. While

these other vulnerabilities could be exploited to provide direct access to servers or immediately unveil encrypted communication, FREAK "only" allows you to significantly weaken the encryption used to protect a single protected "conversation" (session). Attackers still need to break that encryption.
“

This isn't a difficult task for someone experienced in cryptography and

cryptanalysis - or who has access to cryptoanlaytic suites and the experience to properly use such tools. But that added step adds additional work, and likely dissuades attackers from employing it rather than other vulnerabilities whose exploitation offers quicker access to systems or information.
“

FREAK's existence betrays some hard questions that apply far beyond crypto suites. Should we re-invent the wheel by developing new software supposedly without the flaws of yesteryear? Or should we continue to use tried and tested libraries with the knowledge that there could be serious problems either with old exploitable bugs hidden within the software? And even then - when we've made our decision on what technology we should use - how far are we willing to go and how much are we willing to spend to enforce that decision?
“

The last question is the most pertinent for FREAK. The export key lengths exposed via the FREAK vulnerability have been considered insecure for some time now, and neither NIST nor NSA endorse their use given how easy it is to brute force such encryption. But the expense of properly removing these now-insecure encryption schemes can be onerous - as evidenced in the decision by some software vendors not to patch to non-vulnerable versions of SSL and TLS.
“

We're okay with throwing the baby out with the bathwater as an industry. We're not so great at cleaning the tub afterwards.”