ImperialViolet

e POODLE bites again (08 Dec 2014)

October's POODLE attack affected CBC-mode cipher suites in SSLv3 due to SSLv3's under-specification of the contents of the CBC padding bytes. Since SSLv3 didn't say what the padding bytes should be, implementations couldn't check them and that opened SSLv3 up to an oracle attack.

We're done pretty well at killing off SSLv3 in response to that. Chrome 39 (released Nov 18th) removed fallback to SSLv3 and Chrome 40 is scheduled to remove SSLv3 completely. Firefox 34 (released Dec 1st) has already removed SSLv3 support.

We're removing SSLv3 in favour of TLS because TLS fully specifies the contents of the padding bytes and thus stops the attack. However, TLS's padding is a *subset* of SSLv3's padding so, technically, you could use an SSLv3 decoding function with TLS and it would still work fine. It wouldn't check the padding bytes but that wouldn't cause any problems in normal operation. However, if an SSLv3 decoding function was used with TLS, then the POODLE attack would work, even against TLS connections.

This was noted by, at least, Brian Smith on the TLS list ([1][2]) and I was sufficiently cynical to assume that there were probably more instances of this than the old versions of NSS that Brian cited, and so wrote a scanner for the issue.

Unfortunately, I found a number of major sites that had this problem. At least one of whom I had good enough contacts at to quickly find that they used an F5 device to terminate connections. I contacted F5 on October 21st and they started working on a fix. Yngve Pettersen also independently found this issue and contacted me about it around this time.

F5 reported that some of the affected sites weren't customers of theirs, which meant that there was (at least) a

second vendor with the same issue. After more digging, I found that some A10 devices also have this problem. I emailed a number of contacts at A10 on October 30th but sadly didn't get a reply from any of them. It wasn't until November 13th that I found the right person at A10 to deal with this.

F5 have posted patches for their products and A10 should be releasing updates today. I'm not completely sure that I've found every affected vendor but, now that this issue is public, any other affected products should quickly come to light. (Citrix devices have an odd behaviour in this area in that they'll accept padding bytes that are all zeros, but not random padding. That's unexpected but I can't make an attack out of it.)

Ivan Ristić has added a test for this issue to his excellent scanner at SSLLabs. Affected sites will have their grade set to F and will report “This server is vulnerable to the POODLE attack against TLS servers”.

This seems like a good moment to reiterate that *everything* less than TLS 1.2 with an AEAD cipher suite is cryptographically broken. An IETF draft to prohibit RC4 is in Last Call at the moment but it would be wrong to believe that RC4 is uniquely bad. While RC4 is fundamentally broken and no implementation can save it, attacks against MtE-CBC ciphers have repeatedly been shown to be far more practical. Thankfully, TLS 1.2 support is about to hit 50% at the time of writing.