Written by Marco Attard
17 October 2014

Google researchers discover a legacy SSL 3.0 protocol vulnerability, one potentially exposing users of newer Transport Layer Security (TLS) encryption protocols to risk-- Padding Oracle On Downgraded Legacy Encryption, aka POODLE.

Unlike its namesake, POODLE is not too cuddly. Instead, it allows man-in-the-middle attackers to access and read encrypted communications via padding oracle side-channel attack.

SSL 3.0 made its debut back in 1996, but remains a widely used cryptography protocol. Nearly all browsers support it, and use it as a fallback in case of HTTPS server bugs. Thus, network attackers can cause connection failures and trigger SSL 3.0 use in order to exploit the vulnerability.

Google recommends admins disable SSL 3.0 support or CBC-mode ciphers with SSL 3.0. It also suggests the use of the TLS Fallback Signaling Cipher Suite Value (TLS_FALLBACK_SCSV), a mechanism that solves the problems caused by retrying failed connections, as well as prevent downgrades from TLS 1.2 to 1.1 or 1.0.

Meanwhile a Microsoft advisory describes POODLE as "not considered high risk to customers," and Mozilla disabled the use of SSL 3.0 in its Firefox browser.

Go This POODLE Bites: Exploiting the SSL 3.0 Fallback