CS 427, Final Project
POODLE
Padding Oracle on Downgraded Legacy Encryption

Cody Malick
malickc@oregonstate.edu

March 12, 2017

Abstract

This paper outlines the POODLE exploit. It gives details on how it allows an adversary to repeatedly query a server, and eventually decrypt a block one byte at a time. The exploit was first published by the Google Security Team on October 14, 2014 by Bodo Moller, Thai Duong, and Kryzsztof Kotowicz. While SSL version 3.0 is quite old, it is still in use today for browser backward compatibility.

Introduction

Poodle's are cool[1]

The Attack

Context

Padding

AES CBC Mode

Exploit

Exploit Publication by Google

The Fix

Bibliography

References

[1] B. Moller. (2014, October) This poodle bites: exploiting the ssl 3.0 fallback. [Online]. Available: https://security.googleblog.com/2014/10/this-poodle-bites-exploiting-ssl-30.html