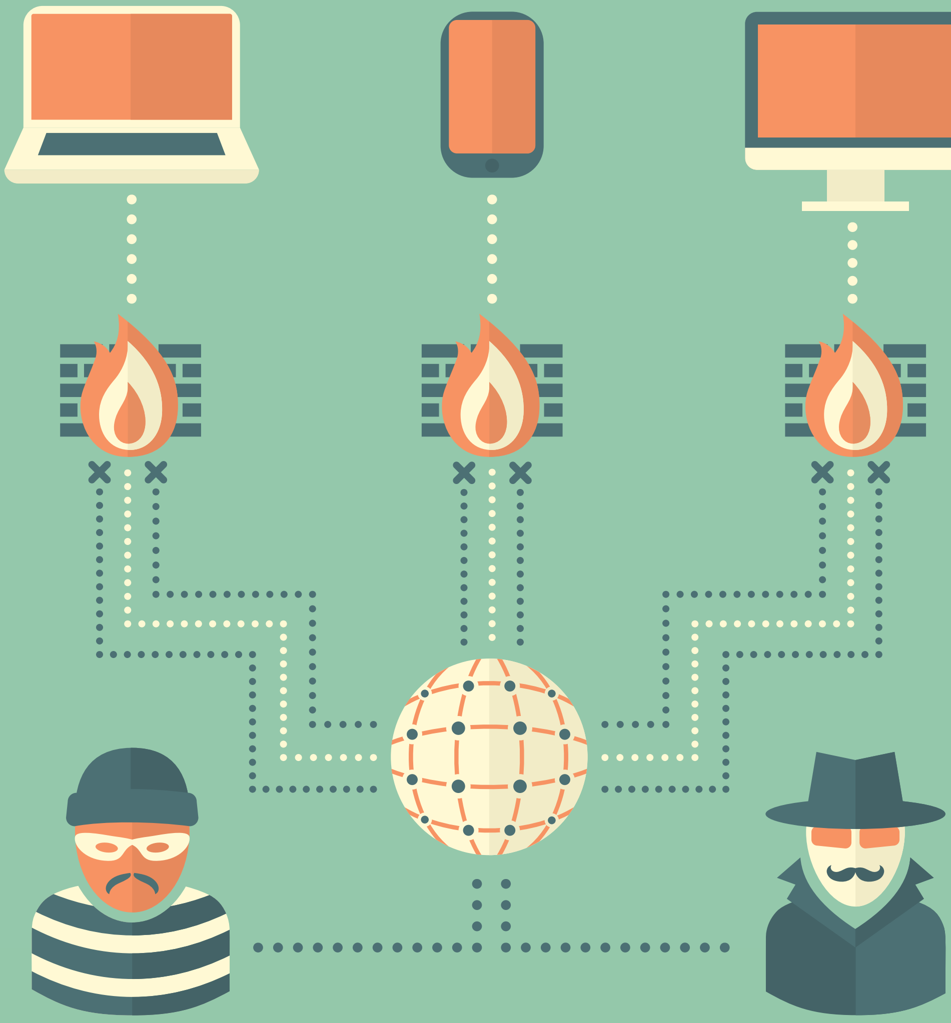
happiest minds

How do you deal with POODLE Vulnerability?



Happiest People . Happiest Customers

Contents

Executive Summary

An unpredicted flaw was discovered in version 3 of the SSL protocol which let attackers to decrypt information that was thought to be transmitted over to a secure HTTPS connection without any discrepancies. This flaw is what's known as POODLE (Padding Oracle on Downgraded Legacy Encryption). What it can do? It can successfully allow attackers to compromise the online-attacks with the greatest ease using a man-in-the-middle attack! This Whitepaper throws light on the nature of POODLE vulnerability and the ways to counter the same using the best practices and recommendations from Happiest Minds.

Description

Initially, information security relied on three basic security principles i.e. confidentiality, integrity and availability. Since the inception of computer networks, cryptographic controls have been used to secure distinct communication channels for data/information exchange. That being said, espionage or theft of corporate information continues to be a real threat even today. As competition is increasingly becoming more and more aggressive, it's essential now, more than ever before, to implement an adequate security control to secure corporate information like Intellectual Property (IPs), Business centric financial data/information, Drug recipe details, Research and Development documents etc. Primarily, Secure Socket Layer (SSL) & Transport Layer Security (TLS) were globally accepted and well known cryptographic protocols which provided adequate assurance level on the confidentiality & integrity related aspects at the time of data / information exchange. Recently, security experts across the globe has discovered that vulnerability into the “SSL version 3” i.e. a cryptography protocol is widely used to implement a secure content transmission. The newly identified vulnerability termed as 'POODLE' (Padding Oracle on Downgraded Legacy Encryption) with severity risk rating, which is set to be “critical” as successful exploitation, could lead to breach confidentiality and integrity of the systems running websites/portals/web applications.

Background Information about POODLE

POODLE stands for Padding Oracle On Downgraded Legacy Encryption, [Padding- A block cipher works on units of a fixed size (known as a block size), but messages come in a variety of lengths. So some modes (namely ECB and CBC) require that the final block be padded before encryption] this vulnerability allows a man-in-the-middle attacker to decrypt cipher-text using a padding oracle side-channel attack. Many Transport Layer Socket (TLS) clients down-grade their cryptography protocol to SSL 3.0 when they work with legacy servers. An attacker that controls the network between the computer and server could interfere with the 'handshake' process, which is used to verify which cryptography protocol the server can accept using a “protocol downgrade dance”. This will force computers to use the older SSL 3.0 protocol to protect data that is being sent. Attackers can then exploit the bug by carrying out a man-in-the-middle (MITM) attack to decrypt secure HTTP cookies, which could let them steal information or take control of the victim’s online accounts.

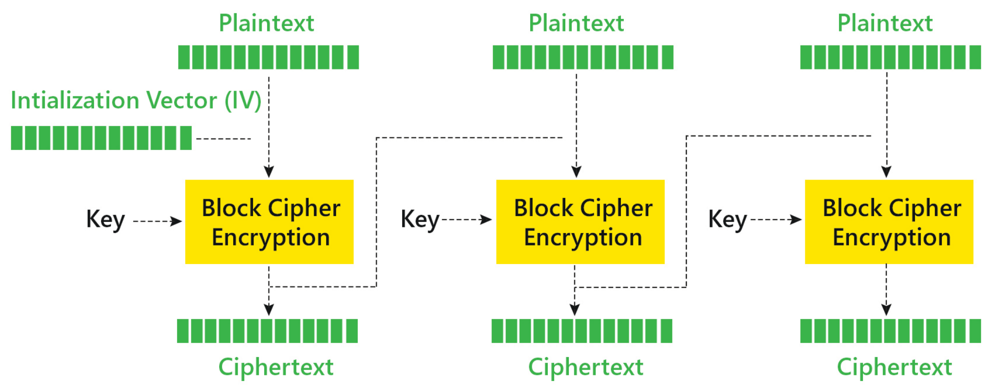
- Note: SSL v3 is an obsolete and insecure protocol. For the most practical purposes now it has been removed by the successor TLS 1.0, TLS 1.1 and TLS 1.2

System Affected

- All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may have a degree of vulnerability. However, POODLE attack demonstrates that this vulnerability, using web browsers and web servers, is one of the most affected.

Cipher-block chaining (CBC)

Cipher-block chaining (CBC) mode of operation in CBC mode, each block of plaintext is XORED with previous ciphertext block before being encrypted. This Way, each ciphertext depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.



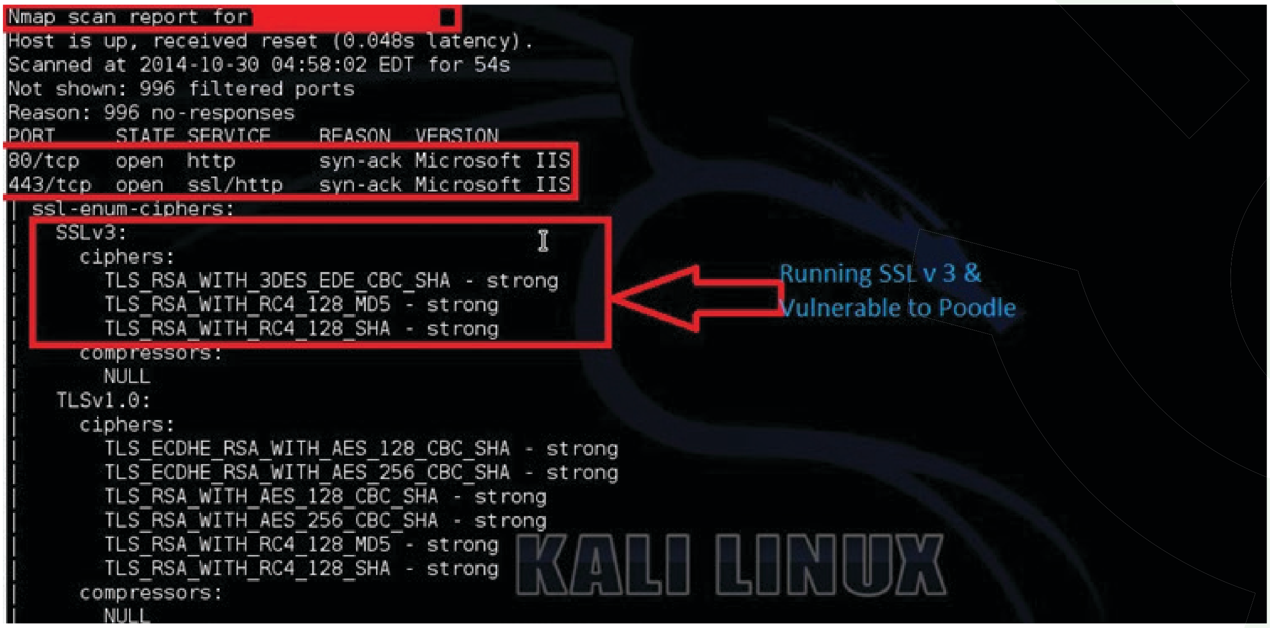
Cipher-block chaining (CBC) mode encryption

Screenshot of POODLE Vulnerability

Affected/Infected Servers

Screenshot #1 - SERVER PRONE TO POODLE VULNERABILITY

In the screen shot below, the SSL v3 is enabled on the server and because of which, it is prone to POODLE vulnerability.

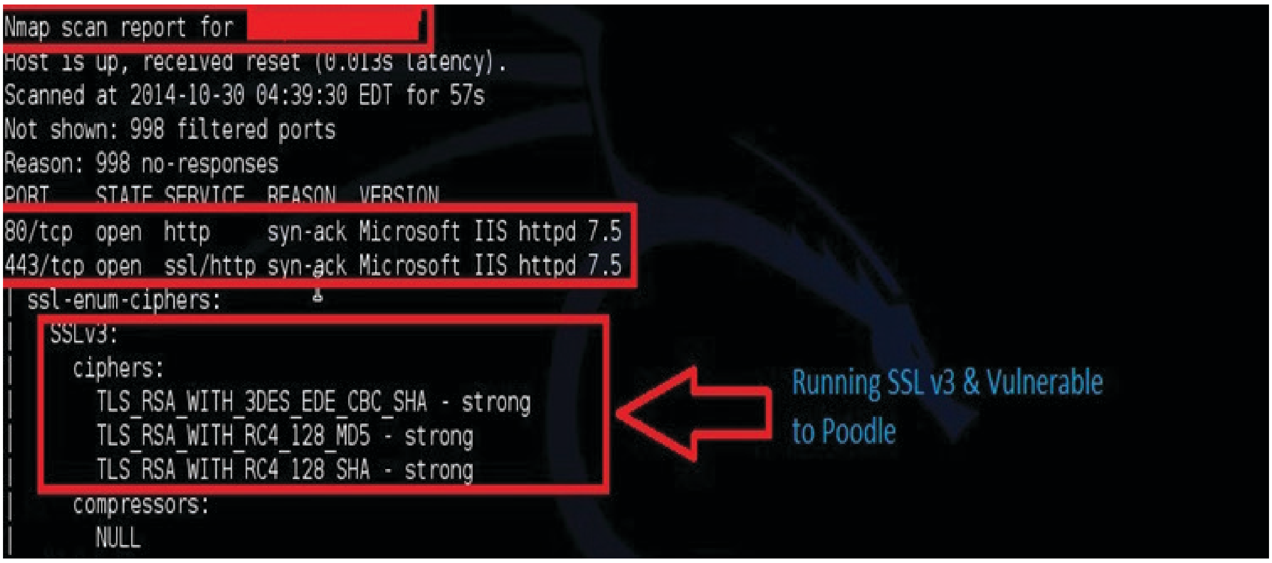


```
Nmap scan report for [redacted]
Host is up, received reset (0.048s latency).
Scanned at 2014-10-30 04:58:02 EDT for 54s
Not shown: 996 filtered ports
Reason: 996 no-responses
PORT     STATE SERVICE    REASON  VERSION
80/tcp   open  http       syn-ack Microsoft IIS
443/tcp  open  ssl/http   syn-ack Microsoft IIS
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
```

Running SSL v 3 & Vulnerable to Poodle

Screenshot #2 - SERVER PRONE TO POODLE VULNERABILITY

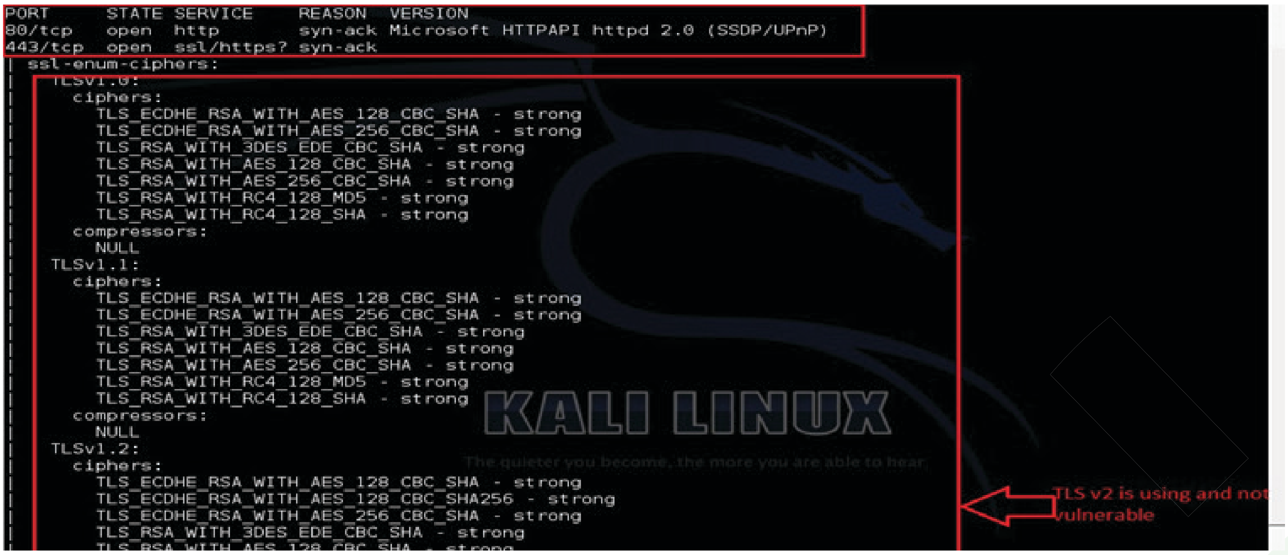
Below server illustrates running with SSL v3 and due to which, it is prone to POODLE vulnerability again.



```
Nmap scan report for [redacted]
Host is up, received reset (0.013s latency).
Scanned at 2014-10-30 04:39:30 EDT for 57s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT    STATE SERVICE  REASON  VERSION
80/tcp  open  http     syn-ack Microsoft IIS httpd 7.5
443/tcp open  ssl/http syn-ack Microsoft IIS httpd 7.5
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
```

Screenshot #3 – SERVER NOT PRONE TO POODLE VULNERABILITY

In the below screen shot, we can see the SSL v3 is not enabled on the server and it employs TLS protocol, making this server not prone to POODLE vulnerability.



```
PORT     STATE SERVICE     REASON  VERSION
80/tcp   open  http        syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  ssl/https?  syn-ack
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_RC4_128_MD5 - strong
|       TLS_RSA_WITH_RC4_128_SHA - strong
|     compressors:
|       NULL
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA - strong
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - strong
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|       TLS_RSA_WITH_AES_128_CBC_SHA - strong
```

Workaround

Man-in-the-Middle Attack

The POODLE attack can be used against any system or application that supports SSL 3.0 with CBC mode ciphers. This not just affects most current browsers and websites, but also includes any software that either references a vulnerable SSL/TLS library or implements the SSL/TLS protocol suite by itself. By exploiting this vulnerability in a likely web-based scenario, an attacker can gain access to sensitive data passed within the encrypted web session, such as passwords, cookies and other authentication tokens that can then be used to gain more complete access to a website (impersonating that user, accessing database content, etc.).

The POODLE attack is a man-in-the-middle exploitation which takes advantage of internet and security software clients which fall back to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. This vulnerability has the CVE ID CVE-2014-3566. POODLE affects older standards of encryption, specifically Secure Socket Layer (SSL) version 3. It does not affect the newer encryption mechanism known as Transport Layer Security (TLS).

Although SSL 3.0 is almost 15 years old, many servers and web browsers are still use it today. When web browsers fail at connecting on a newer SSL version (i.e. TLS 1.0, 1.1, or 1.2), they fall back to a SSL 3.0 connection, which is where the trouble begins. Because a network attacker can cause connection failures, including the failure of TLS 1.0/1.1/1.2 connections, they can force the use of SSL 3.0 and then exploit the poodle bug in order to decrypt secure content transmitted between a server and a browser.

Recommendation

Workaround:

- A workaround has been released from the vendor-end, which says that the SSL V3 should be disabled on the server and enable/allowed either of TLS V1.0,TLS V2.0,TLS V3.0.

- It’s highly recommended to disable the SSLv3.0 on internet facing Business IT applications with higher priority and ensure that they run the required cryptography services on TLS v 1.2 (Transport layer Security).

  Disable SSL 3.0 support in the client.
  Disable SSL 3.0 support in the server.
  Disable support for CBC-based cipher suites when using SSL 3.0 (client & server).

- Similarly, it’s recommended to use the IPS feature of NGFW, (Next Generation Firewall) i.e. by implementing and configuring SSLv3 related IPS signature as a primary counter measure.

- In absence of NGFW, it’s recommended to make use of “Anti-POODLE record splitting” aspects on the respective web server(s) running the vulnerable SSLv3. Further it’s considered as one of the compensatory security controls.

- It’s also recommended to configure “TLS_FALLBACK_SCSV” related parameters on the web-server running with vulnerable SSLv3.

Have a question? Write to us ➔

Author

Karthik Palanisamy

Technical Security Assessment Professional with 4 plus years of consulting experience in network & web application vulnerability assessment and penetration testing, thick client security, database security, mobile application security, SAP application penetration testing, source code audit, configuration review of devices and security architecture review (Applications and Infrastructures).Currently holding a position with Happiest Minds Technologies to deliver technical security assessment and penetration testing services covering application security, infrastructures security, mobile application security and source code review.

About Happiest Minds

Happiest Minds has a sharp focus on enabling Digital Transformation for customers by delivering a Smart, Secure and Connected experience through disruptive technologies: mobility, big data analytics, security, cloud computing, social computing, M2M/IoT, unified communications, etc. Enterprises are embracing these technologies to implement Omni-channel strategies, manage structured & unstructured data and make real time decisions based on actionable insights, while ensuring security for data and infrastructure. Happiest Minds also offers high degree of skills, IPs and domain expertise across a set of focused areas that include IT Services, Product Engineering Services, Infrastructure Management, Security, Testing and Consulting.

Headquartered in Bangalore, India, Happiest Minds has operations in the US, UK, Singapore and Australia. It secured a $52.5 million Series-A funding led by Canaan Partners, Intel Capital and Ashok Soota.

E-mail: Business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on