Systems Affected

All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable. However, the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack demonstrates this vulnerability using web browsers and web servers, which is one of the most likely exploitation scenarios.

Some Transport Layer Security (TLS) implementations are also vulnerable to the POODLE attack.

Overview

CERT is aware of a design vulnerability found in the way SSL 3.0 handles block cipher mode padding. The POODLE attack demonstrates how an attacker can exploit this vulnerability to decrypt and extract information from inside an encrypted transaction.

Description

The SSL 3.0 vulnerability stems from the way blocks of data are encrypted under a specific type of encryption algorithm within the SSL protocol. The POODLE attack takes advantage of the protocol version negotiation feature built into SSL/TLS to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session. The decryption is done byte by byte and will generate a large number of connections between the client and server.

While SSL 3.0 is an old encryption standard and has generally been replaced by TLS, most SSL/TLS implementations remain backwards compatible with SSL 3.0 to interoperate with legacy systems in the interest of a smooth user experience. Even if a client and server both support a version of TLS the SSL/TLS protocol suite allows for protocol version negotiation (being referred to as the “downgrade dance” in other reporting). The POODLE attack leverages the fact that when a secure connection attempt fails, servers will fall back to older protocols such as SSL 3.0. An attacker who can trigger a connection failure can then force the use of SSL 3.0 and attempt the new attack. [1]

Two other conditions must be met to successfully execute the POODLE attack: 1) the attacker must be able to control portions of the client side of the SSL connection (varying the length of the input) and 2) the attacker must have visibility of the resulting ciphertext. The most common way to achieve these conditions would be to act as Man-in-the-Middle (MITM), requiring a whole separate form of attack to establish that level of access.

These conditions make successful exploitation somewhat difficult. Environments that are already at above-average risk for MITM attacks (such as public WiFi) remove some of those challenges.

On December 8, 2014, it was publicly reported [2,3(link is external),4(link is external)] that some TLS implementations are also vulnerable to the POODLE attack.

Impact

The POODLE attack can be used against any system or application that supports SSL 3.0 with CBC mode ciphers. This affects most current browsers and websites, but also includes any software that either references a vulnerable SSL/TLS library (e.g. OpenSSL) or implements the SSL/TLS protocol suite 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.).

Solution

There is currently no fix for the vulnerability SSL 3.0 itself, as the issue is fundamental to the protocol; however, disabling SSL 3.0 support in system/application configurations is the most viable solution currently available.

Some of the same researchers that discovered the vulnerability also developed a fix for one of the prerequisite conditions; TLS_FALLBACK_SCSV is a protocol extension that prevents MITM attackers from being able to force a protocol downgrade. OpenSSL has added support for TLS_FALLBACK_SCSV to their latest versions and recommend the following upgrades: [5]

- OpenSSL 1.0.1 users should upgrade to 1.0.1j.

- OpenSSL 1.0.0 users should upgrade to 1.0.0o.
- OpenSSL 0.9.8 users should upgrade to 0.9.8zc.

Both clients and servers need to support TLS_FALLBACK_SCSV to prevent downgrade attacks.

Other SSL 3.0 implementations are most likely also affected by POODLE. Contact your vendor for details.
Additional vendor information may be available in the National Vulnerability Database (NVD) entry for CVE-2014-3566 [6] or in CERT Vulnerability Note VU#577193.[7]
Vulnerable TLS implementations need to be updated. CVE ID assignments and vendor information are also available in the NVD.[8]

References

- [1] This Poodle Bites: Exploiting The SSL Fallback
- [2] The POODLE Bites Again
- [3] TLS1.x padding vulnerability CVE-2014-8730(link is external)
- [4] A10 Security Advisory(link is external)
- [5] OpenSSL Security Advisory [15 Oct 2014]
- [6] Vulnerability Summary for CVE-2014-3566
- [7] CERT Vulnerability Note VU#577193
- [8] NVD "POODLE TLS" CVE ID Search

Revisions

- October 17, 2014 Initial Release
- October 20, 2014 Added CERT Vulnerability Note VU#577193 to the Solution section
- December 10, 2014 Noted newer POODLE variant (CVE-2014-8730)