VISA SECURITY ALERT

29 October 2014

SSL 3.0 'POODLE' VULNERABILITY

Distribution: Merchants, Issuers, Acquirers, Processors

Who should read this: IT, Information Security, Risk Management

Summary

On October 14, 2014, researchers from Google discovered a critical vulnerability in Secure Sockets Layer version 3.0 (SSL 3.0) (CVE-2014-3566) called POODLE (Padding Oracle On Downgraded Legacy Encryption), also known as POODLEBleed. The SSL 3.0 vulnerability could allow an attacker to carry 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. The attack can be executed both on the server side and client side. Due to the critical nature of this vulnerability, Visa is encouraging clients to update their browsers and disable SSL 3.0 support in system/application configurations.

Description and Impact

The SSL 3.0 vulnerability originates from the way blocks of data are encrypted under the 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.

Transport Layer Security (TLS) (which is not vulnerable in this way) has replaced SSL 3.0 as a legacy encryption standard and most SSL/TLS implementations remain backward compatible with SSL 3.0 to interoperate with legacy systems. The POODLE attack occurs when a secure connection attempt fails and servers fall back to an older protocol, 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.

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, and
2) The attacker must have visibility of the resulting ciphertexts such as through a Man-in-the-Middle (MITM) attack, requiring that level of access.

The POODLE attack can be used against any system or application that supports SSL 3.0. This affects most current Internet 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.). The proliferation of public Wi-Fi and usage of Hotspots makes this attack a serious issue.

Please note that there is a significant likelihood that technology partners and Internet Service providers will stop supporting SSL 3.0. This is why disabling SSL 3.0 and upgrading systems and browsers is strongly recommended.

Mitigation

This Visa Security Alert is provided for information purposes only. Clients and merchants are advised to disable SSL 3.0 support in system/application configurations. While this is the most viable solution, it may cause compatibility issues with customers that use outdated browsers, so Visa recommends testing the behavior of various browsers after removing SSL 3.0 from affected systems.

Older browsers in the corporate and cardholder data environments will also need to be upgraded or modified to disable SSL 3.0. Your browser vendor will have instructions on how best to upgrade or modify a particular browser.

Additional Resources

Further details are provided in the US-CERT alert: https://www.us-cert.gov/ncas/alerts/TA14-290A

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com