TLP: GREEN
October 21,2014
ID# 100202
GSI ID: 1081

SECURITY BULLETIN *POODLE (CVE-2014-3566)*

RISK FACTOR - HIGH

1.1 OVERVIEW / A newly disclosed vulnerability in Secure Socket Layer version 3 (SSLv3) CVE-2014-3566[1] may allow an attacker to calculate the plaintext (cleartext) in secure connections, effectively defeating SSL protection. The SSL security protocol is designed to protect communications on the Internet by wrapping them with encryption to preserve the confidentiality and integrity of communications. It is often used for banking transactions, shopping, secure messaging, instant messaging and email. The vulnerability affects only SSL version 3. It does not affect newer encryption protocols such as Transport Layer Security (TLS).

A proof-of-concept attack called POODLE (Padding Oracle On Downgraded Legacy Encryption) crafted by Google researchers was provided with the vulnerability disclosure.[2] Malicious actors are likely to weaponize and create exploitation tools for the vulnerability. (Please note that the name *padding oracle* has nothing to do with Oracle Corporation or its products; it refers to the target system as an answer-providing oracle.)

This vulnerability may be exploited via man-in-the-middle attacks where a malicious actor will force the fallback (downgrade) of the encryption protocol to SSLv3 and then target the system decrypting the data (the client), observing the exchange and applying a padding oracle attack[3] to recover the plaintext. A more detailed explanation of how these types of attacks work can found on Daniel's Franke blog.[4]

Figure 1 shows a typical SSL handshake between a client and server before data is to be transferred. This handshake has to be established before the POODLE attack takes place, although the attack does not target the handshake.

```
0.386332 X.X.X.X -> Y.Y.Y.Y  SSL 192 Client Hello
0.430303  Y.Y.Y.Y -> X.X.X.X SSLv3 2576 Server Hello, Certificate, Server Key
Exchange, Server Hello Done
0.434186 X.X.X.X -> Y.Y.Y.Y  SSLv3 268 Client Key Exchange, Change Cipher Spec,
Encrypted Handshake Message

0.471297  Y.Y.Y.Y -> X.X.X.X SSLv3 129 Change Cipher Spec, Encrypted Handshake
Message
0.471520 X.X.X.X -> Y.Y.Y.Y  SSLv3 267 Application Data
```

Figure 1: tshark output of an SSLv3 handshake and data transfer

1 *"CVE-2014-3566."* Common Vulnerabilities and Exposures.

2 Möller, Bodo , Thai Duong, and Krzysztof Kotowicz. *"This POODLE Bites: Exploiting The SSL 3.0 Fallback."* Open SSL: Security Advisory. Google, Sept. 2014.

3 Heaton, Robert. "*The Padding Oracle Attack - Why Crypto Is Terrifying.*" Robert Heaton. 29 July 2013.

4 Franke, Daniel Fox. "*How POODLE Happened.*" Indistinguishable from Random. 14 Oct. 2014.

The handshake begins with the client sending a *hello* message to which the server will respond with its own hello message. Once both sides have agreed to encryption terms and completed the handshake process, the encrypted data will begin to transfer. In a web browser, this is the point where a page displays on the screen.

The encrypted web traffic transferred between the client and server, which is called application data, is the data essential to this attack. The attacker could utilize any man-in-the-middle technique to make requests to the victim server and perform a brute-force attack against the encrypted application data to reveal its plaintext variant.

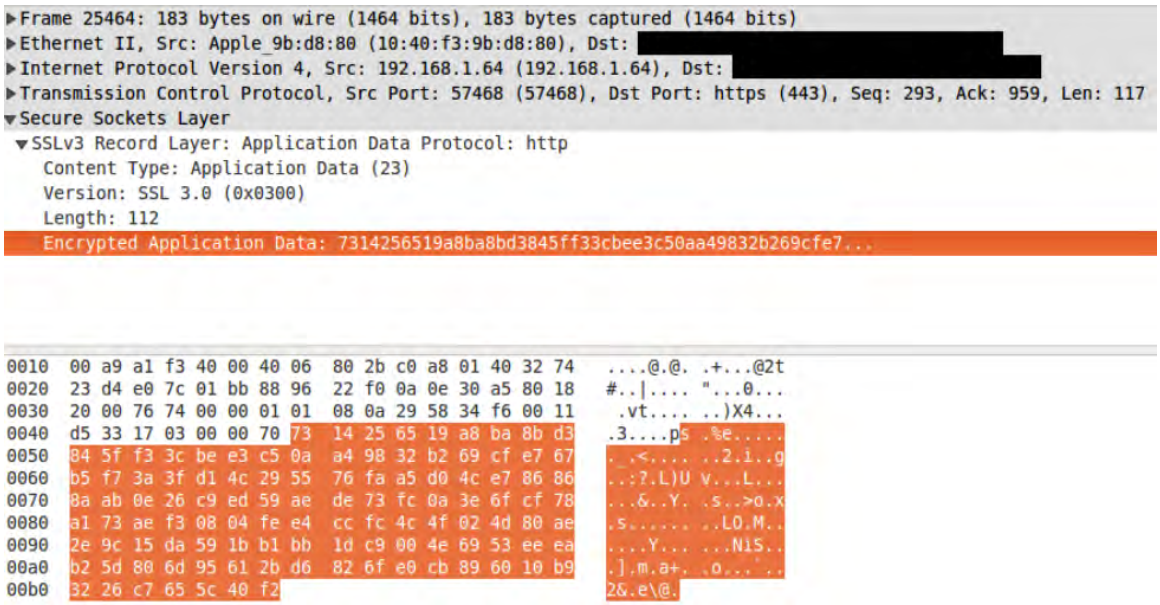

Figure 2: Encrypted application data during SSL-encrypted communication.

1.2 IDENTIFICATION OF RISK / It is important to identify which of your assets could be vulnerable to this type of attack. Server-side testing can be done by confirming cipher suites and supported protocols, using tools such as the following:

- Simple SSL TLS tester from PLXsert can check for the vulnerability quickly across multiple hosts[5]
- SSL Poodle test script from Nmap developers[6]
- POODLE vulnerability test from Tinfoil Security[7]
- SSL server testing service from Qualys SSL Labs[8]

On the client-side, you can use POODLE Test to find out if your browser is susceptible to the attack.[9]

1.3 SYSTEM HARDENING / PLXsert recommends disabling SSLv3 wherever possible. This shouldn't be a problem unless you must support legacy libraries or clients that do not support the TLS protocol.

- Follow the SANS guide to turn off SSLv3 on various servers and clients.[10] It provides concise instructions.
- Apply patches and updates from vendors, especially in cases where SSLv3 can't be disabled.

[5] PLXsert. "*Simple SSL TLS Tester*." GitHub. Akamai, Oct. 2014.
[6] Miller, Daniel."*ssl-poodle NSE script*." Nmap.org.
[7] "*Free POODLE SSL Security Vulnerability Check*." Tinfoil Security.
[8] "*SSL Server Test*." Qualys SSL Labs.
[9] "*POODLE Test*." SSLv3 Poodle Attack Check.
[10] "*POODLE: Turning off SSLv3 for Various Servers and Client*." SANS ISC Community Forums. Oct. 2014.

1.4 ATTACK MITIGATION / The snort rule in Figure 3 detects client connection attempts via SSLv3:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET [443,465,587,995,993] \
(msg:"SSL v3 Client Attempt"; \
flow:to_server; \
ssl_version:sslv3; \
ssl_state:client_hello; \
content:"|16 03 00|"; depth:3; \
classtype:protocol-command-decode; \
sid:201400010;)
```

Figure 3: Snort rule to detect SSLv3 connection attempts

NOTE: The snort rule will detect any client hello messages sent using SSLv3. These may not all be malicious requests. Once SSLv3 is disabled at the infrastructure level, such messages should be limited. The rule can also be used to discover any legacy devices within the infrastructure that are still attempting to connect using SSLv3, alerting to the need for reconfiguration.

The snort rule can be chatty if there are many users still using SSLv3 against a server. A threshold limit can be used to limit log entries to find repeated attempts.[11]

1.5 IMPLICATIONS FOR AKAMAI CUSTOMERS / Detailed information can be found at Akamai's blog "Poodle FAQ: What Akamai's customers need to know." A quick summary includes:

- Akamai has accelerated its deprecation of SSLv3 and earlier versions with a target date if early November.
- Akamai has deployed support for TLS Signaling Cipher Suite Value (SCSV) on the Secure Content Delivery Network (SCDN). SCSV is a cipher suite that prevents downgrading or fallback attacks to SSLv3 or earlier versions in case of a man-in-the-middle attack.
- Akamai is applying the same measures to its internal systems.

[11] "*3.8 Rule Thresholds*." Writing Snort Rules. Snort.org.

The Prolexic Security Engineering and Research Team (PLXsert) monitors malicious cyber threats globally and analyzes these attacks using proprietary techniques and equipment. Through research, digital forensics and post-event analysis, PLXsert is able to build a global view of security threats, vulnerabilities and trends, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, along with best practices to identify and mitigate security threats and vulnerabilities, PLXsert helps organizations make more informed, proactive decisions.

Akamai® is a leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company's solutions is the Akamai Intelligent Platform™ providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 40 offices around the world. Our services and renowned customer care enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on *www.akamai.com/locations*
