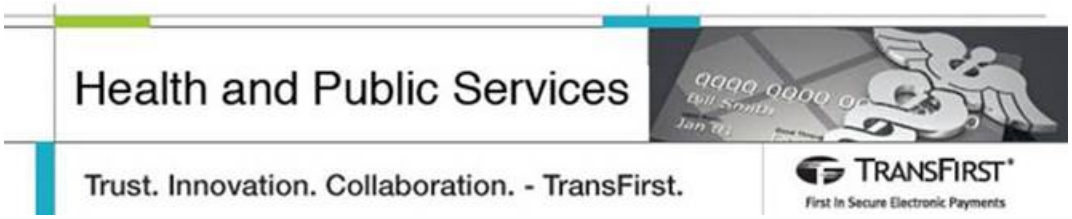
Pia Duryea

From: Hozempa, Sandy <SHozempa@TransFirst.com>
Sent: Monday, March 09, 2015 7:29 PM
Subject: TransFirst Security Alert – POODLE Vulnerability
Attachments: TF4053_Security_POODLE_Insert_v5.pdf



TransFirst Security Alert – SSLv3 aka POODLE Vulnerability

Attention: HPS Sales Partners

How This Affects You: Researchers from Google discovered a vulnerability in Secure Sockets Layer version 3.0 (SSL 3.0) (CVE-2014-3566) called POODLE (Padding Oracle On Downgraded Legacy Encryption). The SSL 3.0 vulnerability could allow an attacker to extract data from secure connections. It has since been determined that the vulnerability also impacts TSL version 1.0.

There is currently no fix for the vulnerability in SSL 3.0 or TSL 1.0 itself, as the issue relates to the design of protocol. This has possible impacts to POS terminals, third party software and our Gateway connections. The specific timing to address required changes is in question as the PCI council is reviewing the impacts on the industry overall. A formal announcement is expected in the next few weeks.

What is TransFirst doing about it?
We have created a statement insert to be received in March (attached) to give merchants notification of possible impacts. Once specific dates are known, we will build off this communication. A copy of the insert included in the February statement received in March is attached.

POS terminals-at this time there are no TSYS certified POS terminal applications that support this new encryption method. The terminal vendors are working diligently to get supporting applications released and TransFirst will do the same once these solutions are available.

Third Party Software-We have completed research with some common vendors used by our merchant base. Most of these vendors already have updated encryption protocol and don't expect any impact. Merchants should reach out to their vendor to ensure they won't have any connectivity issues.

TransFirst Gateways-TC/TXP TCePay- We will be disabling the support of SSLv3 on the test/certification platforms for Transaction Central ePay, Transaction Central Classic and Transaction Express. As part of the

deprecation of SSLv3, TransFirst will also be deprecating support for TLS 1.0 due to risks associated with this version of the cryptographic protocol. This means if a website, shopping cart or integrated software solution uses SSLv3 or TLS 1.0 to send transactions to TransFirst, it will no longer be able to process transactions after these changes are implemented. This is all in preparation for these changes to be rolled out to TransFirst's production environment.

Browser Note for Virtual Terminal access: Most modern browsers are not at risk; if a merchant or partner is using a version of Internet Explorer older than 7.0 they should visit Microsoft's website to update their browser. Firefox, Chrome and Safari users should not be affected by the change.

Software and API Note: Older solutions that use older code or software frameworks that do not support TLS 1.1 or that have disabled TLS, forcing a downgrade to SSLv3, will be affected after these changes are implemented. These solutions will need to upgrade their code base and support TLS 1.1 in order to continue working with TransFirst APIs in the future. For any questions regarding the impact to our Gateways, please contact integrationssupport@transfirst.com.

We will continue to keep you updated on the mandated dates surrounding this issue.

Sandy Hozempa
Director of Operations
TransFirst Health and Public Services
TransFirst, LLC
Direct: 303-625-8156
fax: 303-482-8194

This email transmission and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is the sole property of TransFirst, LLC. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender and destroy and delete all copies of this email and any attachments.