PCI Security Standards Council™

Assessor Update: November 2008

Welcome to the Assessor Newsletter

In This Assessor Update

- **Reporting the use of SSL 2.0 on a Scan Report**
- **Third-parties that receive encrypted cardholder data**
- **PA-DSS Vendor Agreements**

Last week I attended the OWASP European Summit and had the opportunity to speak with several ASVs and QSAs at the event regarding emerging trends in the web application space. The Council is very aware of the increasing threats and will continue to emphasize the importance of security in the development and deployment of the application coding lifecycle. An example of this is the launch of the Payment Application Data Security Standard earlier this year.

As new threats emerge in your application code reviews, we'd love to hear from you. By sharing your discoveries, you can help provide insight that may not be readily available to the Council which in turn helps to shape the requirements, our training and our baselines for testing.

Regards,

Troy Leach

Reporting the use of SSL 2.0 on an ASV Scan Report

During the Community Meeting, a question was asked to the Council regarding the detection of SSL 2.0 during an ASV scan.

Since 2006, the Technical and Operational Requirements for ASVs has stated that an ASV must be able to test for the presences of SSL/TLS and correctly identify version numbers, certificate validity, authenticity and that the certificate matches the server name. The document goes on to say that "a component must be considered non-compliant if the installed SSL version is limited to Version 2.0 or older."

The word "limited" has led some to believe that if, at a minimum, SSL v3.0/TLS v1.0 with 128-bit encryption is installed in conjunction with SSL V 2.0 than that would suffice and a merchant or service provider could still use the less-secure version of the protocol to transmit cardholder data.

The very next sentence however states that "SSL *must* be a more recent version than 2.0" in order to be used to transmit cardholder data as there have been known vulnerabilities in SSL 2.0 for several years.

If we take a step back and look at the intent of the ASV scan, it is to support the continued protection of cardholder data and adherence to all PCI DSS requirements. PCI DSS Requirement 4.1 requires the use of strong cryptography and security protocols to safeguard cardholder data during transmission over public networks, namely the Internet. Strong cryptography and security protocols must be deployed and SSL v3.0/TLS v1.0 should be considered the minimum standard. As such, it is imperative that an ASV identify the use of SSL 2.0 to transmit cardholder data as a failure.

At the same time, we recognize that browser negotiation by the end-user (customer) of the merchant may only have older crypto currently installed. The merchant can enable SSL 2.0 or older for an initial handshake only to identify that the browser requires to be updated. The merchant can then notify their customers that a security update is required in those rare cases prior to making an online purchase using a credit or debit card.

As an ASV, you must determine whether the detection of SSL v2.0 is a false positive or whether they allow for the transmission of cardholder data over a public connection using the older protocol which should not be allowed.

"I not only use all the brains that I have, but all that I can borrow"

– Woodrow T. Wilson

Notices:

The last QSA training of the year is fast approaching in San Francisco. November 20th is the final requalification training and Nov 21st – 22nd will finish the 2008 training for initial qualification training. Check back in early January for the 2009 schedule of training sessions.

Third-parties that receive encrypted cardholder data

Also at the Community Meeting, we discussed the receipt of encrypted cardholder data by a third-party such as an off-site storage location. The question asked was whether the company can be determined to be out of scope of an assessment if they only receive the encrypted data.

The answer is that the organization most likely can be removed from the scope of validation if the merchant or service provider deploys strong cryptography as defined by the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms and the third-party does not have access to the key-encryption key (KEK). The intent is that there is no likely opportunity for the third-party to decrypt the cardholder data to the third party by either manual or automatic methods and that the merchant protects the KEK with appropriate key management as described in Requirement 3.6 of the PCI Data Security Standard.

PA-DSS Vendor Agreement

For PA-QSAs that are speaking to software vendors regarding their role with qualifying a product as PA-DSS compliant, I'd encourage you to share the *Roles and Responsibilities* section from the PA-DSS Program Guide located on the website. I've found this description to be very helpful in both outlining accountability as well as defining the process as it relates to the key players.

Vendors are sometimes confused as to whether they submit attestations, payment application and/or supporting documentation directly to the Council or to their PA-QSA. Vendors should submit their payment applications and supporting documentation to the PA-QSA for review along with permission for their PA-QSA to submit the compliance reports directly to PCI SSC on their behalf once the review is complete.

While the PA-QSA is the conduit to the Council for the report, software vendors still have a direct relationship with the SSC as it pertains to the vendor agreement. The vendor agreement includes such items as the listing fees and responsibilities by the vendor for reporting a compromise. When the application renews, the Council will notify the vendors directly regarding their renewals. As a courtesy, the PA-QSA can also notify their customer but all communication regarding billing will be between the PCI SSC and application vendor. If you haven't done so already, I'd encourage PA-QSAs to read the vendor agreement to better understand the responsibilities of their clients.

Another misconception is about the role of the PA-QSA versus. the role of the Council in reviewing, accepting, and listing the payment application. The PA-QSA's role is to review the application, validate it as compliant, document that compliance in the PA-DSS report, and submit the report and the signed Attestation of Validation to the PCI Council. The Council is then responsible for reviewing the report to confirm quality assurance and accepting the PA-QSA's validation after the vendor agreement has been signed. Only after the vendor agreement has been signed will an application be accepted by the Council and included on the List of Validated Payment Applications.

This is critical to ensure that the vendor understands their continued commitment for the security of the payment application that will be listed.