

## Changes to PCI Security Scan Requirements

---

*June 30, 2008*

Effective June 30, 2008 the PCI Security Standards Council (“PCI SSC”) required Approved Scanning Vendors (“ASV”) to change from version 1 to version 2 of the Common Vulnerability Scoring System (“CVSS”). This change impacts all scanning engines and may impact their customers.

PSC is releasing this bulletin as a continuation of our commitment to help keep our customer informed of security issues and compliance requirements that may impact their business.

### Background

This change impacts the way certain detected vulnerabilities are scored and ranked. Some vulnerabilities that were determined less important under version 1 will receive heightened scoring in version 2. These elevated vulnerabilities may now result in a failing quarterly PCI network scan. This will result in a merchant being non-compliant with the PCI DSS until the vulnerability can be addressed.

PSC’s Scanning Service has been integrating the CVSS 2.0 scoring system since the beginning of 2008. In many cases, vulnerabilities have been scored on the new standard for as long as 6 months. PSC will complete integration testing and have the new scoring standard completely integrated according to the PCI SSC July 1 target.

### Analysis of PCI Issues

Statistically, customer devices may be affected most by these top 5 vulnerabilities:

1. SSL Protocol Version 2 Detection Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.
2. Weak Supported SSL Ciphers Suites The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all. A cipher is considered weak if it is below 128bit encryption.
3. Default Microsoft IIS Files and/or Frontpage Extensions Found Default Files provide a way for an attacker to fingerprint the web server. Previous default IIS files have been known to contain code that could potentially allow an attacker to run arbitrary code on the web server. Frontpage allows remote web developers and administrators to modify web content from a remote location. This provides a serious business risk to the company if left implemented.
4. OpenSSL Multiple Vulnerabilities < 0.9.8d OpenSSL below 0.9.8d is vulnerable to a number of serious vulnerabilities including:

OpenSSL SSLv2 Null Pointer Dereference Client Denial of Service Vulnerability.

OpenSSL SSL\_Get\_Shared\_Ciphers Buffer Overflow Vulnerability.

OpenSSL Insecure Protocol Negotiation Weakness.

OpenSSL Public Key Processing Denial of Service Vulnerability.

OpenSSL DER\_CHOP Insecure Temporary File Creation Vulnerability.

Advanced Encryption Standard Cache Timing Key Disclosure Vulnerability.

OpenSSL PKCS Padding RSA Signature Forgery Vulnerability

OpenSSL is prone to a vulnerability that may allow an attacker to forge an RSA signature. The attacker may be able to forge a PKCS #1 v1.5 signature when an RSA key with exponent 3 is used. An attacker may exploit this issue to sign digital certificates or RSA keys and take advantage of trust relationships that depend on these credentials, possibly posing as a trusted party and signing a certificate or key.

## Recommended Action

All PSC Scan Service accounts have the ability to request an on-demand scan at any time to evaluate their security prior to the customer's next quarterly scan submission date.

### ***PSC Supervised Scanning Customers***

For customers using PSC Supervised Scanning Services, it's as simple as calling the PSC Security Lab to schedule an on-demand scan. Contact the PSC Security Lab at 408-228-0961 x 3. Let our lab know when you want the scan scheduled, and they will take care of the rest. These customers don't need to worry about false-positive analysis or evaluation of scan impact. After the scan is run and analyzed, these customers will receive a report listing any issues. This will be followed up with a debriefing call to help facilitate customer remediation.

### ***Self-Service Scanning Customers (Using PSC Scanning engine)***

PSC recommends that the following steps be taken to execute an on-demand scan:

- Log onto the scan site
- On the left-hand navigation bar, under Security, select "Scans"
- On the breadcrumb trail at the top of the screen, select "On Demand"
- Select the device or devices you wish to scan from the display window, select "Next"
- Leave the Type option set to Hack Simulation
- Leave the Scan Date to Begin or set a scan date
- Now or choose a time up to 24 hours in advance from the drop down box.
- Check the Email When Complete box. Then, if desired, select "Confirm" on the lower right-hand portion of the page.

On Demand scans typically take 3-4 hours to complete. Once the scans are complete, review the reports for issues that need to be resolved.

## More Information

Additional information regarding CVSS and the new scoring criteria can be found here:

<http://www.first.org/cvss/cvss-guide.html>

<http://nvd.nist.gov/cvss.cfm>

If you are a customer of PSC scanning services, contact PSC Security Lab at 408-228-0961 x 3 or your PSC QSA directly. If you're a customer of another scanning company and you need help, PSC Security Labs will support you as well. Just contact PSC at 408-228-0961 x 1 to sign up for help.