PODI dot COM
POTOMAC DIGITEK
online. solved.

Outdated Security Protocols Ending

Credit card processors, e-commerce sites, RSS data feeds, Websites using https, and your browser are all about to change how they communicate with one another. On June 30, 2018, decades-old communication protocols will no longer be supported. And although this transition has been in the works for a long time, you'll be hearing more about it as the June 30, 2018 deadline approaches. Clients conducting PCI scans have already received new messages and warnings that are helping to ensure no one is caught off-guard.

A Brief History

Back in 1990s – in the very early days of the World Wide Web – the Netscape team developed a set of rules for handling sensitive data like credit card numbers. They called this feature a Secure Socket Layer (SSL). As years passed, weaknesses were found and a new set of rules was developed, called Transport Layer Security protocols or TLS.

To ensure online purchases and the exchange of sensitive data could continue without interruption, implementation of TLS included backward compatibility with SSL. When your browser wants to connect to a secure site it initiates a "handshake" during which the browser and server; a) ensure communications are via a legitimate site (using information from the SSL Certificate installed on your website); and b) agree on the level of security protocol to use – settling on a level both parties support.

This has been a good way to ensure secure processing continues to work for a broad set of users, but it also meant clever attackers could circumvent TLS and force the use of older, less secure SSL methods.

In fact, that is what happened when the POODLE and Heartbleed vulnerabilities were exploited back in 2014. Hackers forced a lower security level during the handshake and then gained access to the user's data during the online transaction.

Certificates are not the same as protocols

Before anyone starts worrying that they need to replace their existing SSL Certificates with TLS Certificates, it's important to note that certificates are not dependent on protocols. That is, you don't need to use a TLS Certificate vs. an SSL Certificate. While many vendors tend to use the phrase "SSL/TLS Certificate", it may be more accurate to call them "Certificates for use with SSL and TLS", since the protocols are determined by your server configuration, not the certificates themselves.

It's likely you will continue to see certificates referred to as SSL Certificates because at this point that's the term more people are familiar with, but we're beginning to see increased usage of the term TLS across the industry. SSL/TLS is a common compromise until more people become familiar with TLS.

- GlobalSign Blog

Both vulnerabilities were identified and patches were applied quickly, but it was a stunning warning about the weak security provided by the old rules.

As a result, an effort was started to remove the old rules and replace them with new, more secure, versions. Cryptographic improvements were made and deployed in TLS 1.1 and the current 1.2, but support for TLS 1.0 remained an option in the browser-server handshake.

The only way to remove these old less-secure rules was to drop support for TLS 1.0 and disallow any handshake trying to use them. The challenge is to get all – or at least the majority of – Web users on the same security level.

A deadline of mid-2016 was declared, but not enough of the Web community could be ready by then. The deadline was reset to June 30, 2018, and this time it looks like it will hold. TLS 1.0 will no longer work after that date.

In fact, some companies, like credit card processor Authorize.net, have already made the switch and are no longer supporting TLS 1.0.

What will happen after June 30th?

If you attempt to make an online purchase or complete an ecommerce transaction with an old browser that uses TLS 1.0, the payment process will fail. You will need to upgrade to a newer web browser before completing a purchase under the newer protocols.

NOTE: As of December 2015 all major browsers (Chrome, Firefox, Internet Explorer, Safari and Opera) were already in compliance and supported TLS 1.1 and TLS 1.2.

The Wikipedia page on TLS provides a detailed and comprehensive overview of which browser versions and devices support which security protocols. See Wikipedia: Transport Layer Security for a detailed explanation.

What do you need to do to be prepared?

- ***For Your Web Browser***
  Ensure you are using a modern browser. If you haven't updated your browser software since 2015, you should do so before June 30th. Use this link to check your browser for compliance with TLS 1.1 or TLS 1.2: https://www.howsmyssl.com/

- ***For Your PODI Website***
  We have been working behind-the-scenes since late last year to get all Potomac Digitek hosted websites ready. New software, testing and even a new server are all a part of the effort. As a result, most of our client sites are already compliant. The remainder are on schedule to be compliant by June 30th.

  If your site is regularly scanned for PCI compliance, PODI will provide confirmation that a Risk Mitigation and Migration Plan is in place, and will ensure the migration is completed by the required date.

If you have any questions or concerns regarding the cutoff of TLS 1.0, please contact us so we can respond well in advance of the June 30 deadline.

Other News and Notes

Decorative Plumbing & Hardware Association (DPHA) launched a new website featuring several member-oriented services and directories integrated with the DPHA Filemaker database.

Focusing on employer innovations in health care, a new micro-site spotlights the critical role employers play in the healthcare system by providing comprehensive health coverage at a fraction of the cost to government. Our ***American Benefits Council (ABC)*** client and Mercer (a global leader in the health and benefits marketplace – mercer.com) co-sponsored the new Website.

The ***Property Management Association***'s PMEXPO 2018 - the nation's largest one-day property management tradeshow - will take place Thursday, April 19, 2018 at FedEx Field. A recently launched exhibitor portal, enables registered exhibitors to:

- add product/service listings that appear in the event program
- identify exhibit staff for badging
- purchase exhibit services, i.e. electrical
- add exhibit promotions/discounts

International Society for Pharmacoepidemiology (ISPE) just launched a new micro-site for their mid-2018 meeting. Speakers can upload their bios and presentations. Registrants can view their schedule, contact other attendees, view presentations - from any computer, tablet or phone.

Thank you for your time and look for more valuable tools and tips from Potomac Digitek next month!

Potomac Digitek
820 W. Diamond Ave., Suite 200,
Gaithersburg, MD 20878