ShopSite Knowledgebase

November 13, 2014 email from PayPal regarding POODLE and disabling of SSLv3 on December 3, 2014

Product: ALL
Version: ALL
Platform: ALL
I received an email notification from PayPal stating that on December 3, 2014 they would be disabling the use of SSLv3 on their systems. Does this affect my ShopSite? Is there anything that I need to do?

ShopSite has tested ShopSite 12 against PayPal's test servers that now have SSLv3 disabled and have not encountered any problems.

In addition, since ShopSite v5, the SSL code used by ShopSite is designed to use the newer TLS protocol by default if that is supported on the server ShopSite is securely communicating with (in this case the PayPal servers.)

We do not anticipate any problems when PayPal disables support of SSLv3 on December 3, 2014.
The 11/13/2014 email sent to merchants by PayPal is as follows:

Subject: Immediate Action Required – SSL 3.0 vulnerability

Dear _____,

On Tuesday, October 14, 2014, details were released about a vulnerability to version 3 of Secure Sockets Layer (SSL 3.0). Since that time, PayPal has been hard at work to mitigate any potential impact to our consumers and merchant customers.

To help mitigate risk associated with this vulnerability, PayPal will discontinue support for SSL 3.0 on *December 3, 2014 at 12:01 a.m. Pacific Standard Time. *Unfortunately, this necessary step may cause compatibility problems resulting in the inability for customers to pay with PayPal on your site or other processing issues.

We wouldn't have been able to extend our support of SSL 3.0 to December 3, 2014, at 12:01 a.m. PST if we hadn't also been able to take significant steps to migrate the risk of this vulnerability for our customers. We want to assure our customers we have seen no evidence that the SSL 3.0 issue has led to any compromise of security at PayPal.

Keeping our customers' accounts, data and money secure is PayPal's top priority and a guiding principle when we make challenging decisions, like this one.

We're here to help our merchants through this process. We've put together a comprehensive Merchant Response Guide to ensure systems are secure from this vulnerability.

*What do I need to do? *

**

If you don't manage website integrations for your business, we strongly encourage you to work with your website service partner (developer, hosting company or e-commerce platform, etc.) and share the Merchant Response Guide , which provides the basic guidelines on how to update to Transport Layer Security (TLS). If

your website service has questions or need support, advise them to contact our Merchant Technical Support .

Thank you for your prompt attention to move this issue and understanding of our approach. Though we recognize this necessary step may cause compatibility issues, we can’t stress enough that this short-term inconvenience is heavily outweighed by our joint promise to our respective customers that we will keep their accounts and financial details safe. We plan to keep our customers up to date on how we are addressing this issue via the appropriate channels, including PayPal Forward , our Twitter handle , Customer Service and for merchants, through our Merchant Services team.

For technical assistance, please call 855-489-0342, for quicker routing please contact from a phone number on your PayPal Account. They are available Monday thru Friday from 8:00am to 6:00pm CST.

We appreciate your patience and understanding as we work around the clock to better serve you and keep you and our consumers safe.

Sincerely, GayLynn

https://support.shopsite.com/KBase/questions/2562/