POODLE SSL 3.0 Vulnerability

Payflow Response Guide

Note to Payflow Users

PayPal has recently removed SSL 3.0 support in the Payflow Pilot environment. To verify if your Payflow integration is impacted by the POODLE vulnerability, you can now test your integration against this environment.

1. Test your integration

If you are directly integrated with PayPal Payflow, follow the steps below:

NOTE: If you are integrated through a Partner, we are working with our Partners to resolve the SSL 3.0 issue. If your tests fail, however, we suggest that you reach out to your Partner to report the issue.

a. Point your Payflow Gateway test environment against the Payflow Pilot endpoint: https://pilot-payflowpro.paypal.com

   - SSL 3.0 has already been disabled in the Payflow Pilot environment, so if you can successfully make an application programming interface (API) request you are not using SSL 3.0.

b. If your request fails, check your logs to see why.

   - If you see an error similar to those shown below, then you are using SSL 3.0 and will need to configure your secure connection to use Transport Layer Security (TLS).

```
* Unknown SSL protocol error in connection to pilot-payflowpro.paypal.com:-9824
```

OR

```
140062736746144:error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version
number:s3_pkt.c:337:
...
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol: SSLv3
...
```

OR

```
SSL peer handshake failed, the server most likely requires a client certificate to
connect
```

2. Update to TLS

All Payflow customers are required to disable SSL 3.0 for client interactions as soon as possible and upgrade to TLS. The following table provides basic guidelines on how to update to TLS using common languages and connection methods. Your exact settings may vary…

<table>
<tr><th>Connection Method</th><th colspan="2">Action</th></tr>
<tr><td><b>Payflow SDK</b></td><td colspan="2">If your Java or .NET integration is using the Payflow SDK, we recommend that you test your integration:
• Send a few test transactions to the Payflow Pilot environment, where SSL v3 has been removed, to ensure you will not be impacted. See Step 1 for details.
• If you are unable to process a test transaction due to SSL errors, your server/workstation is not set up to use TLS and you will need to make the appropriate changes to your system.
For information on the latest Payflow SDK versions, see: http://paypal.github.io/sdk/#payflow-gateway
Note: If you are using <b>pfpro.exe</b> or <b>pfpro.dll</b>, you should verify that your application works; if not, contact support for assistance.</td></tr>
<tr><td rowspan="8"><b>API Endpoint</b></td><td colspan="2">Ensure you are connecting to Payflow endpoints using TLS. See the table below to set the TLS protocol for the language you are using. If your environment supports it, do not hardcode to a specific TLS version as the protocol will decide the highest possible version automatically.</td></tr>
<tr><td><b>Language</b></td><td><b>Action</b></td></tr>
<tr><td><b>Ruby</b></td><td>Set the TLS protocol in the OpenSSL::SSL::SSLContext.
• For more details, see: http://ruby-doc.org/stdlib-1.9.3/libdoc/openssl/rdoc/OpenSSL/SSL/SSLContext.html</td></tr>
<tr><td><b>Python</b></td><td>Set the TLS protocol in the ssl.SSLContext.
• For more details, see: https://docs.python.org/2/library/ssl.html#ssl.SSLContext</td></tr>
<tr><td><b>Node.js</b></td><td>Use the correct renegotiation limit as specified here:
• http://nodejs.org/api/tls.html#tls_client_initiated_renegotiation_attack_mitigation</td></tr>
<tr><td><b>PHP</b></td><td>Set CURLOPT_SSLVERSION to CURL_SSLVERSION_TLSv1 in your Curl options.
• For more details, see: http://curl.haxx.se/libcurl/c/CURLOPT_SSLVERSION.html</td></tr>
<tr><td><b>Java</b></td><td>Set the TLS protocol in the javax.net.ssl.SSLContext.
• For more details, see: http://docs.oracle.com/javase/7/docs/technotes/guides/security/jsse/JSSERefGuide.html</td></tr>
<tr><td><b>C#</b></td><td>Use SecurityProtocolType Tls.
• For more details, see: http://msdn.microsoft.com/en-us/library/system.net.securityprotocoltype%28v=vs.110%29.aspx</td></tr>
</table>

3. Evaluate issuing new credentials

After you've successfully tested and upgraded to TLS, you may want to reset your API password (or create an API user if you do not already have an API user created). This step is recommended to help your security, but please make a risk-based decision for your business and customers.

To reset your API password:

a. Log in to the PayPal Manager at https://manager.paypal.com.

b. Click **Account Administration.**

c. Click **Manage Users.**

d. Click the **User Login** that you would like to change the password for:

- Enter the **Admin User Password**.
- Enter a new USER password next to “Reset User Password”.
- Re-enter the new USER password next to “Confirm User Password”.

e. Click **Update**.

NOTE: Please be sure to update your integration with the new password.

To create an API user:

a. Log in to the PayPal Manager at https://manager.paypal.com.

b. Click Account Administration.

c. Click **Add User**.

d. Enter information for all fields denoted by an asterisk.

e. Select a Predefined Role:

- **API_FULL_TRANSACTIONS** – This role is specifically used to process transactions via API, and the user will not be able to login to the PayPal Manager. The user will be able to process all transaction types, including credits, via API.

- **API_LIMITED_TRANSACTIONS** – This user role is specifically used to process transactions via API, and the user will not be able to login to the PayPal Manager. The user will only be able to process non-credit transaction types via API.

f. Click **Update**.

g. Update your integration with the new API user and password.

Thank You

Thank you for your prompt attention to 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 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. We appreciate your patience and understanding as we work around the clock to better serve you and keep you safe.