Dear Cisco Customer,

Cisco engineering has identified the following software issues with the release that you have selected that may affect your use of this software. Please review the Software Advisory notice here to determine if the issues apply to your environment. You may proceed to download this software if you have no concerns with the issue described.

For more comprehensive information about what is included in this software, refer to the Cisco software Release Notes, available from the Product Selector tool. From this page, select the product you are interested in. Release Notes are under "General Information" on the product page.

Reason for Advisory:
This software advisory addresses one software issue.

CSCvh22181
Failures loading websites using TLS 1.3 with SSL inspection enabled

Affected Platforms:
All physical and virtual managed devices, meaning those that run Firepower Threat Defense and ASA with FirePOWER Services

Symptom:
With an SSL inspection policy enabled, TLS 1.3 connections fail for traffic that matches SSL decryption rules.

Starting in March 2018, certain web browsers are being updated to prefer TLS 1.3 traffic over TLS 1.2 traffic. In that case, connections between browsers and websites that support TLS 1.3 fail to establish.

Users see the following error in their browser:

```
ERR_SSL_VERSION_INTERFERENCE
```

In addition, TLS version 1.3 traffic is not decrypted or inspected.

Conditions:
- SSL inspection policy is enabled on the managed device
- TLS 1.3 is enabled in the browser because of a browser update
- The user browses to a web site that supports TLS 1.3

Workaround:
Configure each managed device to remove support for TLS 1.3 and instead negotiate an encrypted connection using TLS 1.2.

On your managed device, use the following steps:

- Log into the CLI using an SSH client to make a connection to the management IP address. Log in using the `admin` username (default password is `Admin123`) or as another CLI user account.

  For more information:
- Firepower Threat Defense devices: Chapter on using the CLI in the *Command Reference for Firepower Threat Defense* for Firepower Threat Defense devices
- Classic devices: "Logging Into the Command Line Interface on Classic Devices" in the *Firepower Management Center Configuration Guide*.
- At the `>` prompt, enter the following command:

  ```
  system support ssl-client-hello-tuning extensions_remove 43
  ```

  (43 is the identifier for the TLS 1.3 protocol.)
- Follow the prompts on your screen to restart the detection engine, Snort. For example:

  ```
  pmtool restartbytype DetectionEngine
  ```

- Enter the following command to confirm the configuration change:

  ```
  system support ssl-client-hello-display
  ```

The following is displayed to confirm the change was successful:
```
extensions_remove=43
```