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.

CSCvj93913
SSL Inspection TLS 1.3 downgrade needs to modify client/server random values to be RFC compliant

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

Symptom:
In Fall 2018, Google releases Chrome 70, which prefers TLS 1.3 connections to Google-managed sites such as Gmail. When that happens, with an SSL inspection policy enabled, TLS 1.3 connections fail for traffic that matches SSL decryption rules.

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 preferred in the browser because of a browser update
- The user browses to a web site, such as Gmail, that supports TLS 1.3

Workaround:

Upgrade your managed device to one of the following releases:

- 6.2.3.1
- 6.2.2.5
- 6.1.0.7

Check this software advisory later for additional patch releases that contain this fix.

We recommend you upgrade your device to the latest available release to get the most features and fixes available.