WSA New Trusted Root Certificate bundle update April 2017

Contents

Introduction

This document describes details about the April 2017 update of the Cisco Trusted Root Bundles and effects on the Cisco Web Security Appliance (WSA).

Background

In effort to keep security of our products at the highest level; Cisco Cryptographic Services team is pleased to announce the release of the next iteration of the Cisco Trusted Root Bundles. This change will also have an effect on WSA. The bundles will be automatically updated on all supported versions of Cisco AsyncOS for Web, and there are no actions needed from WSA administrators.

Update Description

These bundles reflect the latest updates to the bundles derived from upstream trusted root stores as of November 2016.

The most important changes to Cisco Trusted Root Bundles to note:

- Pursuant to the decision of major trust stores (Google, Apple, Mozilla) to remove them, the new Cisco Trusted Root Bundles **no longer contain** roots from **WoSign/StartCom**. Should they resubmit new roots to upstream root stores, we will revisit the decision to remove them from the trust bundles.
- The new Cisco Root CA 2099 has been added to all bundles to support new ACT2 chipsets.
- The old VeriSign root has been replaced in the Core bundle with the newer root that properly chains VeriSign mPKI certificates.
- DST Root CA X1 has been removed from the Core bundle only, as Cisco no longer issues roots from this chain.

What does this mean for WSA users?

- Cisco WSA will download new Root Certificate Bundles using our updater process. No action is needed from WSA Administrators

- If WSA is configured to use decryption, requests towards sites that have SSL certificates signed by **WoSign/StartCom**, will be by default dropped by WSA, as Root CA certificates of this vendor will not be trusted by WSA after the update.
- Alternatively, WSA will apply action configured in HTTPS Proxy -> Invalid Certificate Handling -> Unrecognized Root Authority / Issuer. This action is DROP by default, and Cisco recommends not to change the default Unrecognized Root Authority action.