

Neues Paket für vertrauenswürdige Stammzertifikate für WSA - April 2017

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Beschreibung aktualisieren](#)

[Was bedeutet dies für WSA-Benutzer?](#)

Einleitung

In diesem Dokument werden Details zur Aktualisierung der Cisco Trusted Root-Pakete vom April 2017 und ihren Auswirkungen auf die Cisco Web Security Appliance (WSA) beschrieben.

Hintergrundinformationen

Um die Sicherheit unserer Produkte auf höchstem Niveau zu halten; Das Team von Cisco Cryptographic Services freut sich, die Veröffentlichung der nächsten Version der Cisco Trusted Root Bundles bekannt geben zu können. Diese Änderung wirkt sich auf die WSA aus. Die Pakete werden automatisch für alle unterstützten Versionen von Cisco AsyncOS für Web aktualisiert. Die WSA-Administratoren müssen keine Eingriffe vornehmen.

Beschreibung aktualisieren

Diese Pakete enthalten die neuesten Updates für die Pakete, die ab November 2016 von vertrauenswürdigen Upstream-Root-Stores abgeleitet wurden.

Die wichtigsten Änderungen an Cisco Trusted Root-Paketen:

- Aufgrund der Entscheidung großer Trust Stores ([Google](#), [Apple](#), [Mozilla](#)), diese zu entfernen, enthalten die neuen Cisco Trusted Root Bundles keine Wurzeln mehr aus WoSign/StartCom. Sollten sie neue Roots erneut an Upstream-Root-Stores senden, überdenken wir erneut die Entscheidung, sie aus den Trust-Paketen zu entfernen.
- Die neue Cisco Root CA 2099 wurde allen Paketen zur Unterstützung neuer ACT2-Chipsätze hinzugefügt.
- Der alte VeriSign-Root wurde im Core-Paket durch den neueren Root ersetzt, der VeriSign-mPKI-Zertifikate korrekt kettet.
- Die DST Root CA X1 wurde nur aus dem Core-Paket entfernt, da Cisco keine Roots mehr aus dieser Kette herausgibt.

Was bedeutet dies für WSA-Benutzer?

- Die Cisco WSA lädt neue Stammzertifikatpakete herunter, die unseren

Aktualisierungsprozess verwenden. WSA-Administratoren müssen keine Maßnahmen ergreifen.

- Wenn WSA für die Verwendung von Entschlüsselung konfiguriert ist, werden Anforderungen an Sites mit SSL-Zertifikaten, die von **WoSign/StartCom** signiert wurden, standardmäßig von WSA verworfen, da Stammzertifizierungsstellen dieses Anbieters nach dem Update von WSA nicht mehr als vertrauenswürdig eingestuft werden.
- Alternativ wendet die WSA die unter **HTTPS-Proxy > Invalid Certificate Handling > Unknown Root Authority / Issuer** konfigurierte Aktion an. Diese Aktion ist standardmäßig DROP, und Cisco empfiehlt, die Standardaktion der nicht erkannten Stammzertifizierungsstelle nicht zu ändern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.