

WSA Nieuwe Trusted Root Certificaat Bundle Update - april 2017

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Beschrijving bijwerken](#)

[Wat betekent dit voor WSA-gebruikers?](#)

Inleiding

Dit document beschrijft details over de update van april 2017 van de Cisco Trusted Root Bundles en de gevolgen ervan voor de Cisco Web Security Appliance (WSA).

Achtergrondinformatie

Om de veiligheid van onze producten op het hoogste niveau te houden; Cisco-team voor cryptografische services is verheugd de release van de volgende herhaling van de Cisco Trusted Root Bundles aan te kondigen. Deze verandering zal een effect op WSA hebben. De bundels worden automatisch bijgewerkt op alle ondersteunde versies van Cisco AsyncOS voor Web en er zijn geen acties nodig van WSA-beheerders.

Beschrijving bijwerken

Deze bundels weerspiegelen de nieuwste updates van de bundels die zijn afgeleid van upstream vertrouwde basiswinkels vanaf november 2016.

De belangrijkste wijzigingen in Cisco Trusted Root Bundles:

- In overeenstemming met de beslissing van grote trust stores ([Google](#), [Apple](#), [Mozilla](#)) om ze te verwijderen, bevatten de nieuwe Cisco Trusted Root Bundles geen roots meer van WoSign/StartCom. Mochten zij nieuwe wortels naar upstream root stores, zullen we het besluit om ze uit de trust bundels te verwijderen herzien.
- De nieuwe Cisco Root CA 2099 is toegevoegd aan alle bundels om nieuwe ACT2-chipsets te ondersteunen.
- De oude VeriSign-wortel is in de Core-bundel vervangen met de nieuwere wortel die VeriSign mPKI-certificaten goed ketent.
- DST Root CA X1 is alleen uit de Core-bundel verwijderd, omdat Cisco niet langer wortels uit deze keten uitgeeft.

Wat betekent dit voor WSA-gebruikers?

- Cisco WSA downloadt nieuwe Root Certificate-bundels die ons updateproces gebruiken.

Geen actie van de beheerders van het WSA vereist.

- Als WSA is geconfigureerd voor gebruik van decryptie, zullen aanvragen naar sites die SSL-certificaten hebben ondertekend door **WoSign/StartCom**, standaard worden ingetrokken door WSA, omdat Root CA-certificaten van deze verkoper niet worden vertrouwd door WSA na de update.
- U kunt ook de WSA-toepassing uitvoeren die is geconfigureerd in **HTTPS Proxy > Ongeldige certificaatverwerking > Niet-herkende basisinstantie / afgevende instantie**. Deze actie is standaard beschikbaar en Cisco raadt aan de actie voor de standaard niet-herkende basisinstantie niet te wijzigen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.