

WSA - nieuwe Trusted Root certificaatbundel - april 2017

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Beschrijving bijwerken](#)

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

Inleiding

Dit document beschrijft details over de update in 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 handhaven; Cisco-team voor cryptografische services is verheugd de release van de volgende herhaling van de Cisco Trusted Root-bundels aan te kondigen. Deze wijziging heeft gevolgen voor de WSA. De bundels zullen automatisch worden 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 jongste updates van de bundels die zijn afgeleid van de upstream-wortelwinkels vanaf november 2016.

De belangrijkste wijzigingen in Cisco Trusted Root-bundels ter opmerking:

- Ingevolge het besluit van de grote vertrouwenswinkels ([Google](#), [Apple](#), [Mozilla](#)) om deze winkels te verwijderen, bevatten de nieuwe Cisco Trusted Root-bundels niet langer wortels van WoSign/StartCom. Mochten zij nieuwe wortels opnieuw in de toeleveringsketens leggen, dan zullen we opnieuw het besluit bespreken om die wortels van de vertrouwensbundels te verwijderen.
- De nieuwe Cisco Root CA 2099 is aan alle bundels toegevoegd om nieuwe ACT2-chipsets te ondersteunen.
- De oude VeriSign-wortel is vervangen in de Core-bundel met de nieuwere wortel die VeriSign mPKI-certificaten regelt.
- 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 downloads nieuwe bundels van het Root-certificaat die ons update-proces gebruiken. De WSA-beheerders hoeven geen actie te ondernemen.
- Als WSA wordt geconfigureerd om decryptie te gebruiken, zullen verzoeken naar sites die SSL-certificaten hebben die door **WoSign/StartCom** zijn ondertekend, standaard door WSA worden gedropt, omdat de CA-certificaten van deze verkoper na de update niet door WSA zullen worden vertrouwd.
- Maar WSA zal actie toepassen ingesteld in **HTTPS Proxy > Ongeldige certificaatbehandeling > Niet-herkende wortelinstantie/emittent**. Deze actie is standaard DROP en Cisco raadt aan de standaard niet-herkende actie van de Root Authority te wijzigen.