

Atualização nova do pacote do certificado do root confiável WSA - Em abril de 2017

Índice

[Introdução](#)

[Informações de Apoio](#)

[Descrição da atualização](#)

[Que faz este meio para usuários WSA?](#)

Introdução

Este documento descreve detalhes sobre a atualização de abril de 2017 dos pacotes do root confiável de Cisco e seus efeitos na ferramenta de segurança da Web de Cisco (WSA).

Informações de Apoio

No esforço para manter a Segurança de nossos Produtos no mais de nível elevado; A equipe criptograficamente dos serviços de Cisco é satisfeita anunciar a liberação da iteração seguinte dos pacotes do root confiável de Cisco. Esta mudança terá um efeito em WSA. Os pacotes serão atualizados automaticamente em todas as versões suportadas de Cisco AsyncOS para a Web, e não há nenhuma ação necessária dos administradores WSA.

Descrição da atualização

Estes pacotes refletem as atualizações as mais atrasadas aos pacotes derivados das lojas ascendentes em novembro 2016 do root confiável.

As mudanças as mais importantes ao root confiável de Cisco empacotam para notar:

- Conforme à decisão das lojas principais da confiança ([Google](#), [Apple](#), [Mozilla](#)) para removê-las, os pacotes novos do root confiável de Cisco já não contêm raízes de WoSign/StartCom. Se submeterem novamente raízes novas aos armazenamentos raiz ascendentes, nós revisitaremos a decisão para removê-los dos pacotes da confiança.
- A CA raiz nova 2099 de Cisco foi adicionada a todos os pacotes para apoiar os conjuntos de chip ACT2 novos.
- A raiz velha de Verisign foi substituída no pacote do núcleo com a raiz mais nova essa acorrenta corretamente Certificados do mPKI de Verisign.
- A CA raiz X1 DST foi removida do pacote do núcleo somente, porque Cisco já não emite raízes desta corrente.

Que faz este meio para usuários WSA?

- Cisco WSA transfere pacotes novos do certificado de raiz que usa nosso processo de

atualização. Nenhuma ação é precisada dos administradores WSA.

- Se WSA é configurado para usar a descriptografia, pede para os locais que têm os Certificados SSL assinados por **WoSign/StartCom**, estará deixado cair à revelia por WSA, porque os certificados CA raiz deste vendedor não serão confiados por WSA após a atualização.
- Alternativamente, WSA aplicará a ação configurada no **proxy HTTPS > certificado inválido que segura > autoridade não reconhecida/expedidor da raiz**. Esta ação é GOTA à revelia, e Cisco recomenda não mudar a ação não reconhecida da autoridade da raiz do padrão.