Próxima Mudança na Cadeia de Certificados Let's Encrypt e Impacto para os Clientes

A Let's Encrypt, uma autoridade certificadora (CA) de confiança pública usada pela **Illimitar** para emitir certificados TLS, vinha utilizando duas cadeias de certificados distintas. Uma delas é assinado cruzado com a IdenTrust, uma CA globalmente confiável existente desde 2000, e a outra é a própria CA raiz da Let's Encrypt, ISRG Root X1. Desde o lançamento da Let's Encrypt, a ISRG Root X1 vem conquistando gradativamente compatibilidade com diversos dispositivos.

Em 30 de setembro de 2024, a cadeia de certificados da Let's Encrypt assinada cruzado com a IdenTrust irá expirar. Para se preparar proativamente para essa mudança, desde 2022, a **Illimitar** deixou de emitir certificados da cadeia assinada cruzado e passou a usar a cadeia ISRG Root X1 da Let's Encrypt para todos os futuros certificados Let's Encrypt.

Esta mudança na cadeia de certificados afeta dispositivos e sistemas legados, como dispositivos Android na versão 7.1.1 ou anterior, pois esses dispositivos confiam exclusivamente na cadeia assinada cruzado e não possuem a raiz ISRG X1 em seu armazenamento de confiança. Esses clientes podem encontrar erros ou avisos TLS ao acessar domínios protegidos por um certificado Let's Encrypt.

De acordo com a Let's Encrypt, mais de 93,9% dos dispositivos Android já confiam na ISRG Root X1, e esse número deve aumentar em 2024, especialmente com o lançamento da versão 14 do Android, que facilita a atualização automática do armazenamento de confiança do Android.

Um estudo da Cloudflare analisou alguns dados e descobriu que, de todas as solicitações do Android, 2,96% delas vêm de dispositivos que serão afetados pela mudança. Além disso, apenas 1,13% de todas as solicitações do Firefox vêm de versões afetadas, o que significa que a maioria (98,87%) das solicitações vindas de versões do Android que usam o Firefox não serão impactadas.

Preparando-se para a mudança

Se você está preocupado com a mudança afetando os serviços, há algumas coisas que você pode fazer para reduzir o impacto. Se você controla os clientes que se conectam ao seu aplicativo, recomendamos atualizar o armazenamento de confiança para incluir a ISRG Root X1. Se você usa fixação de certificado, remova ou atualize seu pin. De modo geral, desencorajamos todos os clientes de fixar seus certificados, pois isso geralmente leva a problemas durante renovações de certificado ou mudanças de CA.

Apoiar novos padrões e protocolos de segurança é vital para continuarmos melhorando a internet. Ao longo dos anos, mudanças significativas e, às vezes, arriscadas foram feitas para avançarmos. O lançamento da Let's Encrypt em 2015 foi monumental. A Let's Encrypt permitiu que todo domínio obtivesse um certificado TLS gratuitamente, abrindo caminho para uma internet mais segura, com cerca de 98% do tráfego usando HTTPS atualmente.

Tornando a Infraestrutura de Chave Pública (ICP) Mais Ágil

Para avançarmos no suporte a novos padrões e protocolos, precisamos tornar o ecossistema de Infraestrutura de Chave Pública (ICP) mais ágil. Ao retirar a cadeia assinada cruzado, a Let's Encrypt está incentivando dispositivos, navegadores e clientes a suportarem armazenamentos de confiança adaptáveis. Isso permite que os clientes suportem novos padrões sem causar uma quebra de compatibilidade. Também abre o caminho para o surgimento de novas autoridades certificadoras.

Hoje, uma das principais razões pelas quais há um número limitado de autoridades certificadoras (ACs) disponíveis é que leva anos para que elas se tornem amplamente confiáveis, ou seja, sem assinatura cruzada com outra AC. Em 2017, o Google lançou uma nova AC de confiança pública, o Google Trust Services, que emitia certificados TLS gratuitos. Mesmo tendo sido lançada alguns anos depois da Let's Encrypt, enfrentou os mesmos desafios com compatibilidade de dispositivos e adoção, o que os levou a assinar cruzado com a AC da GlobalSign. Esperamos que, no momento da expiração da AC da GlobalSign, quase todo o tráfego venha de um cliente e navegador modernos, o que significa que o impacto da mudança deverá ser mínimo.

Revisão #: contagem de revisões
Criado: duração de tempo
Atualizado: duração de tempo