استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر – الأسئلة الشائعة

ما هو مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر؟

- مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر (KSK) هو زوج المفتاحين العام والخاص المشفر الذي يلعب دورًا مهمًا في الامتدادات الأمنية لنظام اسم النطاق (DNSSEC). يعمل مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر كنقطة بداية موثوقة للتحقق من صحة DNSSEC، تمامًا كما تعمل منطقة الجذر كنقطة بداية لحل DNS.
- تمامًا كما يبدأ الشخص في منطقة الجذر لحل اسم نطاق في أي مكان في نظام اسم النطاق، فإن البرامج التي تقوم بالتحقق من صحة DNSSEC تثق في مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر وتبني "سلسلة ثقة" من المفاتيح والتوقيعات المتتالية للتحقق من صحة أي بيانات موقعة في نظام اسم النطاق.

ما الذي ينطوي عليه استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر؟

- تستبدل عملية استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر هذه مرساة الثقة الحالية لمنطقة الجذر (KSK-2017) بمرساة ثقة جديدة لمنطقة الجذر (KSK-2024).

لماذا استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر؟

- ليس من الجيد أن يظل مفتاح التشفير قيد الاستخدام لفترة طويلة جدًا. وكأي كلمة مرور، يجب تغييره من حين لآخر.
- من الأفضل إجراء تغييرات استباقية أثناء العمليات العادية عندما تسير الأمور بسلاسة، بدلًا من رد الفعل في حالة الطوارئ.

من يحتاج إلى معرفة أمر استبدال مفتاح توقيع شفرة الدخول الأساسية KSK لمنطقة الجذر؟

- يجب على مزودي خدمة الإنترنت ومشغلي شبكات المؤسسات وغيرهم ممن يقومون بتشغيل التحقق من صحة DNSSEC تحديث أنظمتهم بالجزء العام من مفتاح توقيع شفرة الدخول الأساسية الجديد.

كيف سيعرفون؟

- تقوم مؤسسة ICANN بتنفيذ حملة توعية واسعة النطاق لضمان معرفة من يستخدمون مفتاح توقيع شفرة الدخول الأساسية حاليًا بهذا التغيير.
- يمكن للأطراف المهتمة معرفة المزيد على مواقع ICANN وIANA الإلكترونية، حيث يمكنهم أيضًا متابعة تحديثات مفتاح توقيع شفرة الدخول الأساسية والانضمام إلى قائمة بريدية خاصة. ويمكنهم أيضًا متابعة حسابات ICANN على وسائل التواصل الاجتماعي للبقاء على اطلاع.

ما هو تأثير ذلك على مستخدمي الإنترنت؟

إذا تم إنجاز الأمر بسلاسة، فلن يكون هناك أي تغيير ملحوظ للمستخدمين النهائيين.

ما الذي يمكن أن يحدث خطأً؟

- من المحتمل ألا يتم تحديث بعض البرامج التي تقوم بالتحقق من صحة DNSSEC باستخدام مفتاح توقيع شفرة الدخول الأساسية الجديد، أو أن بعض الأنظمة قد لا تتعامل بشكل صحيح مع التغييرات التي تطرأ على ملف مرساة الثقة المنشور على موقع IANA الإلكتروني.
- إذا انتشرت هذه المشكلات على نطاق واسع، فقد يقرر شركاء إدارة منطقة الجذر عكس التغييرات وإعادة النظام إلى حالة مستقرة. يُعرف هذا باسم "سيناريو التراجع."
- قد يتم أيضًا تعديل الجدول الزمني للاستبدال إذا كانت هناك حاجة إلى وقت إضافي للمساعدة في ضمان استقرار وموثوقية التحقق من صحة DNSSEC أثناء العملية.

ما هو تأثير التراجع أو التمديد؟

- إن الهدف من التراجع أو التمديد هو الحفاظ على الاستقرار التشغيلي، وبالتالي سيكون التأثير على المستخدمين النهائيين ضئيلًا.

كم من الوقت سيستمر التراجع أو التمديد؟

- قد يستمر الأمر إلى أجل غير مسمى أو حتى يتم دراسة الأسباب التي أدت إلى التراجع وتصحيحها. ثم يتم دمج الإصلاحات في عملية جديدة لاستبدال مفتاح توقيع شفرة الدخول الأساسية للجذر.

هل سيشهد مشغلو الشبكات تأثيرًا ماليًا من استبدال مفتاح توقيع شفرة الدخول الأساسية KSK لمنطقة الجذر؟

- في معظم الحالات، ستكون هناك تكلفة صغيرة مرتبطة بالتحضير لاستبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذور. ومع ذلك، يمكن لمشغلي الشبكات الذين لديهم موظفون متخصصون في تكنولوجيا المعلومات المساعدة في التحضير لاستبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر أثناء الصيانة الروتينية للشبكة، دون تكاليف إضافية.
- بعد أن يستعد مشغل الشبكة لاستبدال، من المرجح أن يكون هناك تأثير مالي ضئيل أو معدوم. يمكن لمشغلي الشبكات الذين يتحققون من البنية التحتية لحل نظام اسم النطاق الخاصة بهم دعم التحديث التلقائي للمفتاح ولن يحتاجوا إلى إجراء أي تغييرات على بنيتهم التحتية أو تعديلات على إجراءاتهم التشغيلية.
- إذا لم يكن مشغلو الشبكات مستعدين للاستبدال وقاموا بتمكين DNSSEC، فإنهم يواجهون خطر حدوث تأثير مالي كبير. إذا لم يتم تحديث مرساة الثقة لتعكس المفتاح الجديد، فسوف تتعامل محللات DNS مع الاستجابات الموقعة تحت المفتاح الجديد على أنها قد تم التلاعب بها وستتجاهل تلك الاستجابات. وسيؤدي هذا إلى ظهور خطأ للمستخدمين النهائيين في كل مرة يبحثون فيها عن اسم نطاق، مما قد يؤدي إلى مكالمات دعم من العملاء.

كيف سيتم استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر بالضبط؟

- يتم إجراء استبدال مفتاح توقيع شفرة الدخول الأساسية KSK لمنطقة الجذر تدريجيًا من خلال دورة حياة منظمة ومتعددة المراحل مصممة لضمان استمرارية التحقق من صحة DNSSEC.
- تتكون دورة حياة مفتاح توقيع شفرة الدخول الأساسية من ثماني مراحل على مدى ست سنوات تقريبًا. يظل المفتاح مستخدمًا بشكل فعال للتوقيع لمدة ثلاث سنوات تقريبًا، وترتبط كل مرحلة بمراسم للمفتاح مقررة.
- خلال هذه المراسم، يقوم مفتاح توقيع شفرة الدخول الأساسية بتوقيع مجموعة سجلات موارد (Rrset) المفتاح العام لنظام اسم النطاق DNSKEY لمنطقة الجذر. وتصبح هذه التوقيعات جزءًا من استجابات المفتاح الموقعة، والتي تدعم سلسلة الثقة لـ DNSSEC المستخدمة من قبل محللات التحقق.

ما هو توقيت المراحل الثمانية؟

- تتم عملية الاستبدال بشكل تدريجي متعمد وتمتد لعدة سنوات للمساعدة في ضمان بقاء التحقق من صحة DNSSEC مستقرًا عبر الإنترنت.
- كان KSK-2017 هو مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر النشط منذ عام 2017. وكجزء من عملية الاستبدال، تم إنشاء المفتاح البديل، KSK-2024، في عام 2024 ونشره في منطقة الجذر في فبراير/شباط 2025. ومنذ ذلك الحين، تم نشر كلا المفتاحين بشكل فعال في نظام اسم النطاق تمهيدًا لتولي KSK-2024 مهام التوقيع في 11 أكتوبر/تشرين الأول 2026، مما يمنح محللي التحقق الوقت لتحديث مراسي الثقة الخاصة بهم والاستعداد للانتقال.
- من المخطط حاليًا أن يتم الاستبدال الفعلي – عندما يصبح KSK-2024 هو مفتاح التوقيع النشط الوحيد – في الربع الأخير من عام 2026.
- يصف الجدول الزمني التالي إدخال مفتاح توقيع شفرة الدخول الأساسية البديل، متبوعًا بإخراج مفتاح توقيع شفرة الدخول الأساسية السابق من الخدمة.

المرحلة أ: إنشاء المفتاح (أبريل/نيسان 2024)
يتم إنشاء KSK-2024 في مرفق إدارة المفتاح الأول.
المرحلة ب: نسخ المفتاح (يوليو/تموز 2024)
يتم نسخ KSK-2024 إلى مرفق إدارة المفتاح الثاني. أصبح مفتاح توقيع شفرة الدخول الأساسية الآن مؤهلًا لدخول مرحلة الإنتاج.
المرحلة ج: يتم توقيع البيانات الأولى باستخدام KSK-2024 لاستخدامها في **المرحلة د** (أكتوبر/تشرين الأول 2024)
يتم توقيع المجموعة الأولى من طلبات توقيع المفتاح.
المرحلة د: النشر (فبراير/شباط 2025)
يتم نشر KSK-2024 في منطقة الجذر.
يتم استخدام كل من KSK-2017 و KSK-2024 لتوقيع منطقة الجذر.
المرحلة هـ: الاستبدال (الربع الرابع من 2026)
يتم استخدام KSK-2024 فقط لتوقيع منطقة الجذر.
المرحلة و: الإلغاء (الربع الأول من 2027)
يتم إزالة KSK-2017 من منطقة الجذر.
المرحلة ز: الحذف 1 (الربع الثاني من 2027)
يتم حذف KSK-2017 من مرفق إدارة المفتاح الأول.
المرحلة ح: الحذف 2 (الربع الثالث من 2027)
يتم حذف KSK-2017 من مرفق إدارة المفتاح الثاني.

ما الإجراء الذي يمكن اتخاذه الآن؟

- ينبغي على مطوري البرامج الذين يقومون بإنشاء أو صيانة برامج التحقق من صحة DNSSEC التأكد من أنها تتوافق مع RFC 5011.
- بالنسبة للبرامج التي لا تتوافق مع RFC 5011، أو البرامج التي تم تكوينها لعدم استخدام RFC 5011، سيكون ملف مرساة الثقة لتدفق النشر متاحًا على موقع IANA الإلكتروني. يجب استرداد الملف عند بدء تشغيل المحلل، وعند تغيير مفاتيح KSK في DNSKEY RRset في منطقة الجذر لنظام اسم النطاق.
- يمكن لمطوري البرامج ومشغلي محللات التحقق الوصول إلى الاختبارات التشغيلية التي طورتها ICANN لتقييم ما إذا كانت أنظمتهم تنفذ RFC 5011 بشكل صحيح وسيتم تحديثها تلقائيًا أثناء عملية استبدال مفتاح توقيع شفرة الدخول الأساسية لمنطقة الجذر.

كيف يمكنني المشاركة؟

اطرح سؤالًا
أرسل بريدًا إلكترونيًا إلى globalsupport@icann.org مع كتابة "استبدال مفتاح توقيع شفرة الدخول الأساسية" في خانة الموضوع لإرسال أسئلتك.

انضم إلى قائمة مناقشة استبدال مفتاح توقيع شفرة الدخول الأساسية
اشترك في القائمة البريدية للمشاركة في المناقشات العامة حول القضايا ذات الصلة.