Let’s Encrypt, la popular autoridad de firma de certificados gratuita. va a revocar más de 3 millones de certificados TLS en las próximas 24 horas, esto debido a un error.

El error ocurrió en su software de Autoridad de Certificación. El cual confirmó el 29 de febrero. Afecto la forma en que verificó la propiedad del nombre de dominio antes de dar nuevos nuevos certificados TLS.

El error generó un escenario en el que se podía emitir un certificado incluso sin validar adecuadamente el control del titular de un nombre de dominio.

Una política de seguridad de Internet, Autorización de la Autoridad de Certificación (CAA), accede que los titulares de nombres de dominio, puedan indicar a las autoridades de certificación (CA) si están autorizados o no para poder emitir certificados digitales para un nombre de dominio específico.

Los resultados de validación de dominio por Let’s Encrypt , son válidos solo durante 30 días, desde el momento en que se de la validación. Después de lo cual vuelve a comprobar el registro CAA que autoriza ese dominio antes de emitir el certificado.

Let’s Encrypt dijo que el 2,6 por ciento de aproximadamente 116 millones de certificados activos están afectados, alrededor de 3.048.289. Una gran cantidad.

Asì que el error, se diò de la siguiente manera, en el código de Boulder, el software de firma de certificados utilizado por Let’s Encrypt. Boulder elegía un nombre de dominio y lo verificaba N veces, cuando una solicitud de certificado contenía N nombres de dominio que necesitaban volver a comprobar CAA. Se introdujo en una actualización en julio de 2019.

Let’s Encrypt podría haber emitido certificados que no debió tener en primer lugar; por lo cual está revocando. Ya que se estánn duplicando.

Es importante destacar, que lo propietarios de sitios web afectados tienen hasta las 8 p.m. UTC (3 p.m. EST) del 4 de marzo para renovar y reemplazar manualmente sus certificado.

En este caso, los certificados emitidos por Let’s Encrypt son válidos por un período de 90 días, y los clientes de ACME como Certbot son capaces de renovarlos automáticamente. Con Let’s Encrypt revocando todos los certificados afectados, los administradores del sitio web deberán realizar una renovación forzada para evitar interrupciones. Además se debe usar la herramienta https://checkhost.unboundtest.com/ para verificar si un certificado necesita reemplazo

Para apoyo de los suscriptores, Let’s Encrypt ha reunido una lista descargable de números de serie afectados, lo que permite verificar si sus sitios web dependen de un certificado afectado.