La autoridad de certificación (CA) DigiCert ha anunciado que revocará un grupo específico de certificados SSL/TLS en las próximas 24 horas debido a un error en la verificación de si un certificado digital se emite al propietario legítimo de un dominio.

La empresa indicó que procederá a revocar los certificados que no tengan una validación de control de dominio (DCV) adecuada.

> *«Antes de emitir un certificado a un cliente, DigiCert valida el control o la propiedad del cliente sobre el nombre de dominio para el cual están solicitando un certificado utilizando uno de varios métodos aprobados por el Foro CA/Browser (CABF)»*, mencionó la empresa.

Una de las maneras de realizar esta validación es solicitando al cliente que configure un registro DNS CNAME que contenga un valor aleatorio proporcionado por DigiCert, quien luego realiza una búsqueda DNS para el dominio en cuestión para asegurar que los valores aleatorios coincidan.

Según DigiCert, este valor aleatorio se prefija con un carácter de subrayado para evitar posibles colisiones con subdominios reales que utilicen el mismo valor aleatorio.

Lo que la compañía, con sede en Utah, descubrió es que en algunos casos de validación basados en CNAME, no se incluyó el prefijo de subrayado en el valor aleatorio.

El problema tiene su origen en una serie de cambios implementados desde 2019 para renovar la arquitectura subyacente, en el cual se eliminó el código que añadía un prefijo de subrayado y posteriormente *«se añadió a algunas rutas en el sistema actualizado»* pero no a una ruta específica que no lo añadía automáticamente ni verificaba si el valor aleatorio tenía un subrayado pre-apendizado.

> *«La omisión de un prefijo de subrayado automático no fue detectada durante las*

> *revisiones del equipo multifuncional realizadas antes del despliegue del sistema actualizado»,* dijo DigiCert.
>
> *«Aunque teníamos pruebas de regresión, esas pruebas no nos alertaron sobre el cambio en la funcionalidad porque se enfocaban en los flujos de trabajo y la funcionalidad, en lugar del contenido/estructura del valor aleatorio.»*
>
> *«Desafortunadamente, no se hicieron comparaciones entre las implementaciones de valores aleatorios heredados y las del nuevo sistema para cada escenario. Si hubiéramos hecho esas evaluaciones, habríamos descubierto antes que el sistema no estaba agregando automáticamente el prefijo de subrayado al valor aleatorio donde era necesario.»*

Posteriormente, el 11 de junio de 2024, DigiCert dijo que renovó el proceso de generación de valores aleatorios y eliminó la adición manual del prefijo de subrayado dentro del marco de un proyecto de mejora de la experiencia del usuario, pero reconoció que nuevamente fallaron en *«comparar este cambio de UX con el flujo de subrayado en el sistema heredado.»*

La compañía explicó que no descubrió el problema de incumplimiento hasta *«hace varias semanas»* cuando un cliente no identificado se puso en contacto sobre los valores aleatorios utilizados en la validación, lo que llevó a una revisión más profunda.

También indicó que el incidente afecta aproximadamente al 0.4% de las validaciones de dominio aplicables, lo que, según una actualización en el informe relacionado de Bugzilla, afecta a 83,267 certificados y 6,807 clientes.

Se recomienda a los clientes notificados que reemplacen sus certificados lo antes posible iniciando sesión en sus cuentas de DigiCert, generando una Solicitud de Firma de Certificado (CSR) y reemitiéndolos después de pasar la DCV.

Este desarrollo llevó a la Agencia de Seguridad de Infraestructura y Ciberseguridad de los EE. UU. (CISA) a publicar una alerta, indicando que *«la revocación de estos certificados puede causar interrupciones temporales en sitios web, servicios y aplicaciones que dependen de estos certificados para la comunicación segura.»*