

Boletín de alerta

Boletín Nro.: 119

Fecha de publicación: 21/10/2026

Tema: Alerta 2026-119 Compromiso de CA intermedias de eMudhra afecta la confianza en conexiones TLS

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La exposición depende del almacén de confianza utilizado por cada proceso, no solamente del sistema operativo.

Tecnología o ambiente	Riesgo que debe revisar el administrador	Acción principal
Servidores Linux y clientes basados en OpenSSL/GnuTLS	Herramientas y servicios pueden continuar confiando en las cadenas afectadas a través del almacén del sistema.	Actualizar ca-certificates mediante el proveedor y verificar el resultado.
Windows y Windows Server	Equipos aislados o con actualizaciones automáticas de certificados deshabilitadas podrían no haber recibido el bloqueo de Microsoft.	Comprobar la distribución de listas de confianza y desconfianza; gestionar bloqueos corporativos cuando corresponda.
Python y aplicaciones que incorporan certifi	Cada entorno virtual o aplicación puede contener su propio conjunto de raíces.	Actualizar certifi y el software que lo incluya; la versión 2026.10.19 incorpora la corrección.
Node.js, Go y Java	Los runtimes o binarios pueden utilizar raíces propias o mecanismos distintos de validación.	Revisar actualizaciones y almacenes efectivos. El seguimiento lista Node.js 22.23.4, 24.22.1 y 26.12.1, y Go 1.27.3 y 1.26.10 como corregidos; Java continúa pendiente en esa matriz.
Contenedores e imágenes base	Un host actualizado no corrige los certificados incluidos dentro de las imágenes.	Actualizar imágenes, reconstruirlas y reemplazar las instancias desplegadas.

Aplicaciones con certificados integrados

Herramientas como clientes cloud, aplicaciones de escritorio y controladores pueden conservar copias independientes.

Actualizar cada producto y verificar sus bundles de certificados.

Herramientas de línea de comandos en macOS

Algunas herramientas utilizan /etc/ssl/cert.pem o almacenes propios sin aprovechar los bloqueos del sistema.

Validar cada cliente; no asumir que el bloqueo de Apple cubre todas las herramientas.

Descripción

Se confirmó el compromiso de las claves privadas de ocho autoridades certificadoras intermedias de eMudhra: seis destinadas a certificados TLS y dos a firma de código. Una generación incorrecta de las claves permite recuperarlas a partir de los certificados públicos, situación existente desde su creación en abril de 2025. Un atacante con estas claves podría generar certificados fraudulentos que determinados clientes acepten como legítimos. Aunque los principales navegadores y plataformas ya distribuyeron bloqueos, servidores, herramientas de línea de comandos, contenedores y aplicaciones con almacenes de certificados propios pueden continuar expuestos si no reciben las actualizaciones correspondientes.

Descripción: qué es una CA y por qué este incidente importa

Una autoridad certificadora —CA, por *Certificate Authority*— emite certificados digitales que permiten verificar identidades. En HTTPS/TLS, el certificado vincula un nombre de dominio con una clave pública; el cliente valida su firma y la cadena que lo conecta con una CA en la que confía.

La cadena habitual tiene tres niveles:

- CA raíz: representa un punto de confianza instalado en el sistema, navegador o aplicación.
- CA intermedia: recibe autoridad de una raíz u otra CA para emitir certificados.
- Certificado del servicio: identifica al sitio o servidor con el que se establece la conexión.

En este incidente se comprometieron claves de CA intermedias, no simplemente la clave de un sitio web. Por ello, el problema no queda limitado a una organización o dominio: un atacante podría emitir certificados para suplantar servicios ante clientes que todavía acepten esas cadenas. Los certificados afectados encadenan a raíces reconocidas por los programas de confianza de Mozilla, Microsoft, Apple y Chrome, además de numerosos almacenes derivados.

El compromiso tampoco significa que el atacante pueda descifrar automáticamente cualquier conexión HTTPS. Para interceptar una sesión necesitaría, además de un certificado aceptado por el cliente, una posición que le permita redirigir o intervenir la conexión. El certificado fraudulento podría hacer que esa suplantación no genere el error de identidad que normalmente debería detenerla.

Qué ocurrió y qué protecciones existen

El investigador que notificó el problema demostró posesión de las ocho claves mediante firmas sobre un mensaje y comunicó el incidente a los programas de confianza el 17 de octubre. Según el seguimiento público, los certificados quedaron bloqueados en Firefox y Chrome desde el 17, en dispositivos Apple desde el 19 y en plataformas Microsoft desde el 20. La CA también revocó los certificados intermedios comprometidos.

Sin embargo, revocar un certificado no garantiza que todos los clientes dejen de aceptarlo. Muchos programas fuera del navegador no consultan información de revocación o utilizan almacenes propios que requieren actualización independiente. Este es el principal riesgo residual para los administradores.emudhra.

El seguimiento del incidente indica que no se encontraron entradas de Certificate Transparency —CT— para estas intermedias desde su creación. Según ese análisis, los navegadores que exigen CT no habrían aceptado certificados fraudulentos emitidos por ellas durante ese período. Esta protección no debe extrapolarse a clientes que no aplican CT; se desconoce si las claves fueron utilizadas para atacarlos.

El principal riesgo es la **suplantación** de sitios, APIs y servicios mediante certificados fraudulentos que algunos clientes todavía podrían aceptar como legítimos. Si un atacante consigue redirigir o interceptar la conexión, podría capturar credenciales, tokens o información sensible y modificar las respuestas del servicio. El compromiso de las claves no permite descifrar automáticamente todo el tráfico HTTPS: también requiere intervenir la conexión y que el cliente confíe en la cadena afectada.emudhra.

En servidores, contenedores y procesos de CI/CD, el riesgo puede persistir aunque el navegador o el sistema operativo ya estén actualizados, porque algunas aplicaciones utilizan almacenes de certificados independientes. Esto podría facilitar la manipulación de descargas o comunicaciones automatizadas cuando no existan verificaciones adicionales de firma o integridad. Además, dos intermedias comprometidas corresponden a firma de código, por lo que también debe comprobarse que las plataformas rechacen esas cadenas; aceptar una firma fraudulenta no implica, por sí solo, la ejecución automática del archivo.

Solución

La solución consiste en distribuir las actualizaciones que eliminen o bloqueen la confianza en las cadenas comprometidas, tanto en el sistema operativo como en cada aplicación que mantenga su propio almacén. Actualizar únicamente el navegador no corrige necesariamente los clientes de servidor.

1. Inventariar almacenes de confianza del sistema, runtimes, entornos virtuales, contenedores y aplicaciones.
2. Aplicar las actualizaciones oficiales de certificados y productos.
3. Comprobar especialmente equipos Windows desconectados o sujetos a políticas que impidan recibir las listas de certificados.
4. Reconstruir y desplegar imágenes de contenedores con los componentes actualizados.
5. Si no existe corrección del proveedor, evaluar el bloqueo administrado de las cadenas afectadas. Retirar raíces completas puede interrumpir conexiones legítimas, por lo que requiere pruebas y

control de cambios.emudhra.we-have-a-problem+1

6. No utilizar `-insecure`, `verify=False` ni deshabilitar la validación TLS para resolver los errores que aparezcan tras el bloqueo.

Verificación de exposición

El sitio de seguimiento ofrece dos endpoints de prueba:

curl https://dv-g3b-emudhra.we-have-a-problem.com/

curl https://dv-g3b-aaa-emudhra.we-have-a-problem.com/

Un rechazo explícito por validación del certificado indica que ese cliente rechaza la cadena presentada.

Una conexión exitosa sin errores indica que debe investigarse su confianza en esa cadena. Un timeout, error DNS o bloqueo de red no demuestra protección.

La prueba debe repetirse con los clientes y entornos relevantes: que curl rechace la conexión no demuestra que Java, Python, Node.js o una aplicación empaquetada también lo hagan. Estos dos endpoints tampoco constituyen una validación exhaustiva de todas las intermedias y rutas de confianza comprometidas.

Información adicional:

- Seguimiento del incidente, certificados afectados y matriz de correcciones:
<https://emudhra.we-have-a-problem.com>
- RFF — evaluación de Linux, Windows y almacenes integrados:
<https://getrff.com/blog/emudhra-compromise-linux-servers/>