El fabricante de software para escritorio remoto AnyDesk anunció el viernes que fue víctima de un ciberataque que resultó en el compromiso de sus sistemas de producción.

La empresa alemana afirmó que el incidente, descubierto durante una auditoría de seguridad, no constituye un ataque de ransomware y que ya ha informado a las autoridades pertinentes.

> *«Todos los certificados relacionados con la seguridad han sido revocados, y se han aplicado medidas correctivas o reemplazado sistemas según sea necesario. En breve, revocaremos el certificado de firma de código anterior para nuestros archivos ejecutables y ya hemos comenzado el proceso de sustitución por uno nuevo»,* declaró la compañía en un comunicado.

Como medida preventiva, AnyDesk también invalidó todas las contraseñas de su portal web, my.anydesk[.]com, instando a los usuarios a cambiar sus contraseñas si las mismas se utilizaban en otros servicios en línea.

Además, se recomienda a los usuarios que descarguen la versión más reciente del software, la cual incluye un nuevo certificado de firma de código.

AnyDesk no proporcionó detalles sobre cuándo ni cómo se produjo la brecha en sus sistemas de producción. Actualmente, se desconoce si se sustrajo alguna información tras el ataque. No obstante, se enfatizó que no hay pruebas de que los sistemas de los usuarios finales se hayan visto afectados.

A principios de esta semana, Günter Born de BornCity informó que AnyDesk estuvo en mantenimiento desde el 29 de enero, y la situación se resolvió el 1 de febrero. Previamente, el 24 de enero, la empresa también alertó a los usuarios sobre *«interrupciones intermitentes»* y *«degradación del servicio»* en su Portal de Cliente.

AnyDesk cuenta con más de 170,000 clientes, entre ellos Amedes, AutoForm Engineering, LG

Electronics, Samsung Electronics, Spidercam y Thales.

Este anuncio se produce un día después de que Cloudflare revelara que fue comprometido por un presunto atacante respaldado por un estado, quien utilizó credenciales robadas para obtener acceso no autorizado a su servidor de Atlassian y, finalmente, acceder a parte de la documentación y una cantidad limitada de código fuente.