Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERATAQUE A ANYDESK: IMPORTANTE PROVEEDOR DE ACCESO REMOTO CONFIRMA BRECHA DE SEGURIDAD

31 / 01 / 2024

CONTENIDO

INTRODUCCIÓN

AnyDesk, un destacado proveedor de soluciones de acceso remoto, ha confirmado ser víctima de un reciente ciberataque que comprometió sus sistemas de producción. Durante el incidente, los hackers accedieron al código fuente y las claves de firma de código privado, generando preocupaciones sobre la seguridad de sus 170,000 clientes, entre ellos importantes empresas como 7-Eleven, Comcast, Samsung, MIT, NVIDIA, SIEMENS y las Naciones Unidas. Aunque AnyDesk asegura que la situación está bajo control y no hubo ransomware, se insta a los usuarios a actualizar a la última versión con un nuevo certificado de firma de código.

CIBERATAQUE A ANYDESK: IMPORTANTE PROVEEDOR DE ACCESO REMOTO CONFIRMA BRECHA DE SEGURIDAD

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_02_02_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	02/02/2024
Es día cero (0 day):	No

RESUMEN

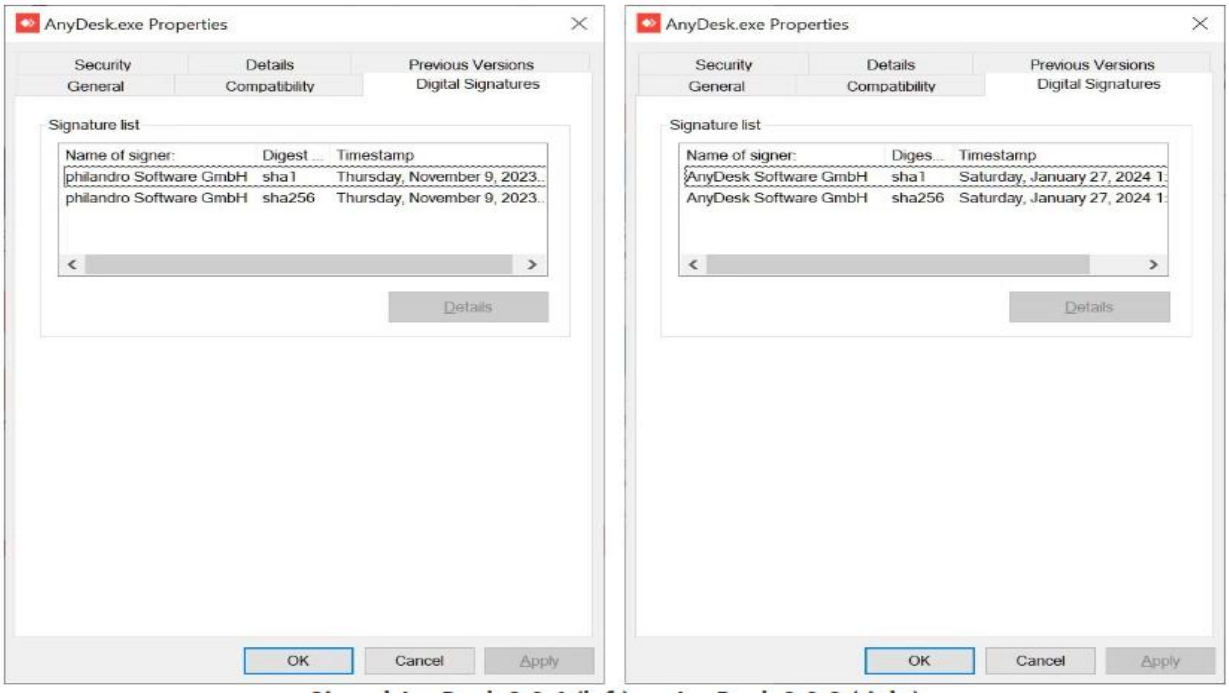
AnyDesk, un destacado proveedor de soluciones de acceso remoto ha confirmado hoy que fue víctima de un reciente ciberataque que comprometió sus sistemas de producción. Durante el incidente, los hackers lograron acceder al código fuente y las claves de firma de código privado de la empresa, lo que plantea preocupaciones sobre la seguridad de sus 170,000 clientes, incluyendo empresas líderes como 7-Eleven, Comcast, Samsung, MIT, NVIDIA, SIEMENS y las Naciones Unidas.

La empresa reveló que se percataron del ataque después de detectar señales de un incidente en sus servidores de productos. Tras una auditoría de seguridad, confirmaron la violación y activaron un plan de respuesta en colaboración con la firma de ciberseguridad CrowdStrike.

Aunque AnyDesk no proporcionó detalles específicos sobre la cantidad de datos robados, se sabe que los atacantes se hicieron con el código fuente y los certificados de firma. La compañía aseguró que no hubo ransomware involucrado y que la situación está bajo control, pero ha instado a los usuarios a actualizar a la última versión del software con un nuevo certificado de firma de código.

AnyDesk también confirmó que no se robaron tokens de autenticación de sesión, pero por precaución, están revocando todas las contraseñas del portal web. A pesar de afirmar que los dispositivos de los usuarios finales no se vieron afectados, la compañía recomienda cambiar las contraseñas, especialmente si se utilizan en otros sitios.

Günter Born de BornCity informó que la compañía ha iniciado el reemplazo de los certificados de firma de código comprometidos, reflejado en la versión 8.0.8 del software lanzada el 29 de enero. Este cambio es vital para garantizar la integridad y seguridad del servicio.



AnyDesk 8.0.6 (izquierda) frente a AnyDesk 8.0.8 (derecha)

El mantenimiento reciente en el portal web de AnyDesk, que duró cuatro días a partir del 29 de enero, estuvo relacionado con el incidente de ciberseguridad, según confirmó la empresa. Aunque el acceso se ha restablecido, se aconseja encarecidamente que todos los usuarios actualicen el software y cambien sus contraseñas para garantizar una mayor seguridad.

Este ataque a AnyDesk se suma a la creciente lista de infracciones contra empresas de renombre, destacando la importancia crítica de la seguridad cibernética en la era digital actual. La compañía, junto con otras afectadas recientemente como Cloudflare y Microsoft, demuestra la necesidad constante de estar alerta y tomar medidas proactivas para proteger la información y los sistemas contra amenazas cibernéticas en evolución constante.

NOTICIA COMPLETA

https://devel.group/blog/ciberataque-a-anydesk-importante-proveedor-de-acceso-remoto-confirma-brecha-de-seguridad/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente