# Incidente de seguridad en AnyDesk

CYBERZAINTZA-AVISOS

**TLP: CLEAR**

www.ciberseguridad.eus

## TABLA DE CONTENIDO



## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## 1. Resumen ejecutivo

El 2 de febrero, el fabricante de software de escritorio remoto **AnyDesk**, ha publicado un aviso sobre un **incidente de seguridad** que ha descubierto tras una auditoría.

Este incidente ha **comprometido los sistemas de producción, el código fuente y las certificaciones de firma de código** del software.

**AnyDesk** ha activado un **plan de reparación y respuesta,** en el que ha participado la compañía de ciberseguridad Crowdstrike, tomando las medidas correspondientes tales como reemplazar los sistemas comprometidos y asegurar la integridad de la versión más reciente del software.

Además, la firma ha alertado a todos sus usuarios y ha publicado una serie de recomendaciones.

## 2. Recursos afectados

- Cualquier versión anterior a AnyDesk 8.0.8

## 3. Análisis técnico

**AnyDesk**, tras recibir indicios de compromiso en algunos de sus sistemas de producción, ha realizado una auditoría de seguridad y ha encontrado pruebas de que el **código fuente y las claves de firma de código privado han sido comprometidas.**

La compañía está reemplazando los certificados de firma de código comprometidos, **lanzando la versión 8.0.8 del software** el pasado 29 de enero, cambio necesario para asegurar la integridad y seguridad del servicio. Para ello ha sido necesario una **interrupción de servicio de cuatro días,** durante los cuales los usuarios no han podido iniciar sesión.

Aunque el proveedor no ha proporcionado detalles de los datos comprometidos, ha confirmado que **no se han robado tokens de autenticación de sesión**, pero que, por precaución, están revocando todas las contraseñas del portal web. A su vez, tampoco tiene evidencia de que, hasta la fecha, los dispositivos de usuarios finales hayan sido comprometidos.

## 4. Mitigación / Solución

Para prevenir cualquier incidente, se recomienda utilizar la última versión del software con el nuevo certificado de firma de código. Así mismo, **AnyDe**sk recomienda **cambiar la contraseña**, sobre todo, si esta está siendo utilizada en otros sitios.

Se recuerda que **AnyDesk** es una herramienta lícita de control remoto de equipos y que puede convertirse en un **vector de entrada silencioso si no se actualiza a la última versión.**

## 5. Referencias Adicionales

- https://anydesk.com/en/public-statement


cyber
zaintza
BASQUE CYBERSECURITY AGENCY