Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ALERTA DE CONNECTWISE: VULNERABILIDADES CRÍTICAS EN SCREENCONNECT

31 / 01 / 2024

CONTENIDO

INTRODUCCIÓN

La empresa ConnectWise ha lanzado una advertencia urgente a sus clientes sobre una vulnerabilidad crítica en su software ScreenConnect, que podría permitir a los atacantes realizar ejecuciones remotas de código (RCE). Esta debilidad de seguridad, relacionada con un bypass de autenticación, podría comprometer servidores y exponer datos confidenciales. Aunque no hay evidencia de explotación en la naturaleza, la compañía insta a los administradores a aplicar parches inmediatamente. Huntress, un equipo de investigación de seguridad ha creado un exploit de prueba de concepto para demostrar la gravedad del problema. Además, las agencias de seguridad han alertado sobre el aumento del uso malicioso de software de administración remota, como ScreenConnect, destacando la importancia de abordar estas vulnerabilidades críticas.

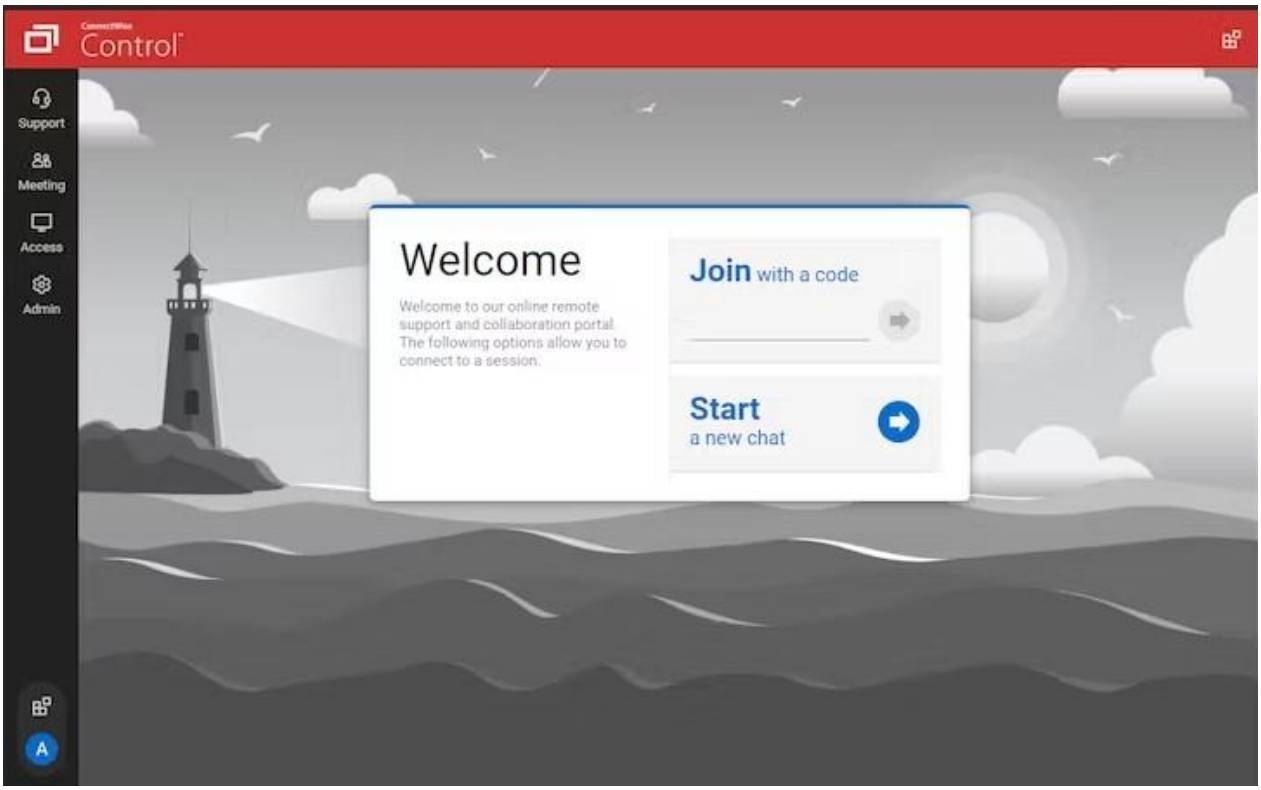
ALERTA DE CONNECTWISE: VULNERABILIDADES CRÍTICAS EN SCREENCONNECT

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:	21/02/2024
Es día cero (0 day):	No

RESUMEN

ConnectWise ha emitido una advertencia urgente a todos los administradores de ScreenConnect para que parcheen de inmediato sus servidores debido a una vulnerabilidad crítica que podría ser explotada para realizar ataques de ejecución remota de código (RCE). Esta vulnerabilidad, que afecta a las versiones anteriores a la 23.9.8 de ScreenConnect, se debe a una vulnerabilidad de bypass de autenticación que permite a los atacantes acceder a datos confidenciales o ejecutar código malicioso en los servidores vulnerables sin necesidad de interacción por parte del usuario.



Además de esta falla crítica, ConnectWise también ha solucionado un problema de vulnerabilidad de recorrido de ruta en su software de escritorio remoto. Aunque esta vulnerabilidad solo puede ser aprovechada por atacantes con altos privilegios, es esencial abordarla para garantizar la seguridad de los servidores afectados.

ConnectWise ha instado a todos los usuarios de ScreenConnect a actualizar sus servidores a la última versión disponible lo antes posible para mitigar estos riesgos de seguridad. Aunque no hay evidencia de explotación en la naturaleza hasta el momento, es fundamental tomar medidas preventivas para proteger los sistemas contra posibles ataques.

Los investigadores de seguridad de Huntress han confirmado la existencia de un exploit de prueba de concepto (PoC) para eludir la autenticación en servidores de ScreenConnect no parcheados. Esta vulnerabilidad podría ser aprovechada por actores de amenazas para llevar a cabo ataques en una amplia variedad de organizaciones que utilizan ScreenConnect en sus operaciones.

La importancia de este parche se destaca aún más en el contexto de un reciente aviso conjunto emitido por CIS, la NSA, y MS-ISAC, que advierte sobre el aumento del uso de software de monitoreo y administración remota (RMM) con fines maliciosos por parte de los atacantes. Es esencial que las organizaciones tomen medidas proactivas para proteger sus sistemas contra posibles ataques y asegurar la integridad de sus datos y operaciones.

NOTICIA COMPLETA

https://devel.group/blog/alerta-de-connectwise-vulnerabilidades-criticas-en-screenconnect/

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