Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CISA advierte a las organizaciones que cambien a Exchange Online Modern Auth hasta octubre.

29/junio/2022

Contenido

INTRODUCCIÓN

Por medio del presente boletín, queremos notificarle sobre las ultimas recomendaciones que la agencia CISA a brindado al publico en general (sector Publico y Privado) sobre los cambios y buenas practicas en servidores Exchange.

EXCHANGE

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

ID de alerta:	DSOC-CERT_2022_06_29_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	06/29/2022
Es día cero (0 day):	NO

RESUMEN

CISA ha instado a las agencias gubernamentales y organizaciones del sector privado que utilizan la plataforma de correo electrónico en la nube Exchange de Microsoft para acelerar el cambio de los métodos de autenticación heredados de autenticación básica sin soporte de autenticación multifactor (MFA) a las alternativas de autenticación moderna.

La autenticación básica (autenticación de proxy) es un esquema de autenticación basado en HTTP que utilizan las aplicaciones para enviar credenciales en texto sin formato a servidores, terminales o servicios en línea.

La alternativa, Modern Auth (Biblioteca de autenticación de Active Directory y autenticación basada en tokens de OAuth 2.0), utiliza tokens de acceso de OAuth con una vida útil limitada que no se pueden reutilizar para autenticar en otros recursos además de aquellos para los que fueron emitidos.

Las aplicaciones que utilizan autenticación básica permiten a los atacantes adivinar las credenciales en ataques de difusión de contraseñas o capturarlas en ataques de intermediarios a través de TLS. Para empeorar las cosas, cuando se usa la autenticación básica, la autenticación multifactor (MFA) es bastante complicada de habilitar y, como resultado, a menudo no se usa en absoluto.

Se necesita con urgencia un conmutador de autenticación moderno

También se aconsejó a las agencias de la Rama Ejecutiva Civil Federal (FCEB, por sus siglas en inglés) que bloquearan la autenticación básica después de migrar a la autenticación moderna, lo que, según Microsoft, hará que sea más difícil para los actores de amenazas realizar ataques exitosos de rociado de contraseñas y relleno de credenciales.

De acuerdo con la guía de CISA, esto se puede hacer creando una política de autenticación para todos los buzones de correo de Exchange Online desde la página de autenticación moderna del Centro de administración de M365 (detalles aquí) o una política de acceso condicional en Azure Active Directory (AAD) usando el Centro de administración de AAD (instrucciones aquí).

"Aunque esta guía está diseñada para las agencias de FCEB, CISA insta a todas las organizaciones a cambiar a Modern Auth antes del 1 de octubre Y HABILITAR MFA ".

La autenticación básica se desactivará en octubre

La advertencia de CISA se produce después de que Microsoft TAMBIÉN RECORDARÁ A los clientes en mayo que comenzará a deshabilitar la autenticación básica en inquilinos aleatorios en todo el mundo a partir del 1 de octubre de 2022.

Microsoft anunció por primera vez que deshabilitaría la autenticación básica en Exchange Online para todos los protocolos en todos los inquilinos en septiembre de 2021.

"Hemos deshabilitado la autenticación básica en millones de inquilinos que no la estaban usando, y actualmente estamos deshabilitando los protocolos no utilizados dentro de los inquilinos que aún lo usan, pero cada día que su inquilino tiene habilitada la autenticación básica, está en riesgo de sufrir un ataque. ", dijo la empresa.

Redmond planea deshabilitar la autenticación básica para los protocolos MAPI, RPC, Libreta de direcciones sin conexión (OAB), Servicios web de Exchange (EWS), POP, IMAP y PowerShell remoto.

Si bien SMTP AUTH ya se ha deshabilitado en millones de inquilinos que no lo estaban usando, Microsoft dijo que no lo deshabilitará donde todavía esté en uso.

Amit Serper, vicepresidente ejecutivo de investigación de seguridad de Guardicore en ese momento, reveló CÓMO CIENTOS de miles de credenciales de dominio de Windows se filtraron en texto sin FORMATO A dominios externos por parte de clientes de correo electrónico mal configurados que usaban autenticación básica.

Recomendaciones

1. Si usted utiliza los servicios de Exchange, valide todo se encuentre funcionando de forma adecuada, y prepare un plan de acción para aplicar las medidas indicadas en este boletín.

Noticia Completa

https://www.bleepingcomputer.com/news/security/cisa-warns-orgs-to-switch-to-exchange-online-modern-auth-until-october/

Enlaces de Importancia

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication#directly-blocking-legacy-authentication

https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

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