Investigadores de seguridad cibernética revelaron una vulnerabilidad sin parches en el protocolo utilizado por Microsoft Azure Active Directory, que los adversarios potenciales pueden utilizar para organizar ataques de fuerza bruta no detectados.

> *«Esta falla permite a los actores de amenazas realizar ataques de fuerza bruta de un solo factor contra Azure Active Directory (Azure AD) sin generar eventos de inicio de sesión en el inquilino de la organización objetivo»*, dijeron los investigadores de Secureworks Counter Threat Unit (CTU) en un informe publicado este miércoles.

Azure Active Directory es la solución de gestión de acceso e identidad (IAM) empresarial basada en la nube de Microsoft, diseñada para el inicio de sesión único (SSO) y la autenticación de múltiples factores. También es un componente central de Microsoft 365, con capacidades para proporcionar autenticación a otras aplicaciones a través de OAuth.

La vulnerabilidad reside en la función de inicio de sesión único sin interrupciones que permite a los empleados firmar automáticamente cuando usan sus dispositivos corporativos que están conectados a redes empresariales sin tener que ingresar ninguna contraseña. El SSO sin interrupciones también es una *«característica oportunista»* en el sentido de que si el proceso falla, el inicio de sesión vuelve al comportamiento predeterminado, en el que el usuario debe ingresar su contraseña en la página de inicio de sesión.

Para lograr esto, el mecanismo se basa en el protocolo Kerberos para buscar el objeto de usuario correspondiente en Azure AD y emitir un ticket de concesión de tickets (TGT), que permite al usuario acceder al recurso en cuestión. Sin embargo, para los usuarios de Exchange Online con clientes de Office anteriores a la actualización de Office 2013 de mayo de 2015, la autenticación se realiza a través de un punto final basado en contraseña llamado *«UserNameMixed»* que genera un token de acceso o un código de error dependiendo de si las credenciales son válidas.

Son estos códigos de error de donde proviene la falla. Aunque los eventos de autenticación exitosos crean registros de inicio de sesión al enviar los tokens de acceso, *«la autenticación*

de Autologon en Azure AD no se registra», lo que permite aprovechar la omisión para ataques de fuerza bruta no detectados a través del punto de conexión UserNameMixed.

Secureworks dijo que notificó a Microsoft sobre el problema el 29 de junio, solo para la compañía reconociera el comportamiento el 21 de julio como *«por diseño».*

Microsoft también aclaró que las mitigaciones contra ataques de fuerza bruta ya se aplican a los puntos finales antes mencionados, y que los tokens emitidos por la API UserNameMixed no brindan acceso a los datos, agregando que deben presentarse nuevamente a Azure AD para obtener los tokens reales. Dichas solicitudes de tokens de acceso están protegidos por acceso condicional, Azure AD autenticación de múltiples factores, Azure AD protección de la identidad, y aparecieron en el inicio de sesión en los registros.