Investigadores en ciberseguridad han identificado una vulnerabilidad de seguridad «crítica» en la implementación de la autenticación multifactor (MFA) de Microsoft. Esta falla permite que un atacante evada con facilidad la protección y obtenga acceso no autorizado a la cuenta de una víctima.

> *«La omisión fue sencilla: tomó aproximadamente una hora realizarla, no requería ninguna acción por parte del usuario, no generaba alertas ni notificaba al titular de la cuenta sobre la intrusión»,* explicaron los expertos de Oasis Security, Elad Luz y Tal Hason, en un informe.

Tras un proceso de divulgación responsable, Microsoft corrigió el problema, conocido como AuthQuake, en octubre de 2024.

Microsoft ofrece varios métodos para autenticar usuarios mediante MFA. Uno de ellos requiere que, tras ingresar las credenciales, el usuario introduzca un código de seis dígitos generado por una aplicación de autenticación. Se permite un máximo de 10 intentos fallidos consecutivos dentro de una sola sesión.

La vulnerabilidad señalada por Oasis se debe principalmente a la ausencia de un límite de intentos y a un intervalo de tiempo prolongado para generar y validar estos códigos de un solo uso. Esto posibilita que un atacante cree numerosas sesiones rápidamente y pruebe todas las combinaciones posibles del código (es decir, hasta un millón) sin que la víctima reciba notificaciones sobre los intentos fallidos.

Es importante destacar que estos códigos, conocidos como contraseñas de un solo uso basadas en el tiempo (TOTP, por sus siglas en inglés), se generan utilizando la hora actual como referencia. Además, tienen una vigencia limitada de aproximadamente 30 segundos, después de los cuales son reemplazados por un nuevo código.

> *«No obstante, debido a posibles desfases horarios o retrasos entre el usuario y el*

> *sistema validador, este último suele aceptar un margen de tiempo más amplio para validar los códigos. En resumen, un código TOTP puede ser válido durante más de 30 segundos»,* mencionaron los investigadores de Oasis.

En el caso de Microsoft, Oasis descubrió que los códigos podían considerarse válidos durante hasta 3 minutos. Esto brindaba una oportunidad para que los atacantes aprovecharan ese margen ampliado para realizar múltiples intentos de fuerza bruta simultáneos y descifrar el código de seis dígitos.

> *«Es esencial establecer límites de velocidad y garantizar que se implementen correctamente. Además, los intentos fallidos consecutivos deberían activar un mecanismo de bloqueo en la cuenta»*, afirmaron los investigadores.

Microsoft ha introducido desde entonces un límite de velocidad más riguroso, que se activa después de varios intentos fallidos. Según Oasis, este nuevo límite permanece vigente durante unas 12 horas.

> *«El descubrimiento de la vulnerabilidad AuthQuake en el sistema MFA de Microsoft nos recuerda que la seguridad no consiste solo en implementar MFA, sino también en configurarlo correctamente»*, declaró James Scobey, director de seguridad de la información en Keeper Security.
>
> *«Si bien MFA es una herramienta altamente efectiva, su éxito depende de configuraciones clave, como los límites de velocidad para evitar ataques de fuerza bruta y las notificaciones al usuario sobre intentos de inicio de sesión fallidos. Estas características no son opcionales; son fundamentales para mejorar la detección temprana de actividad sospechosa y permitir una respuesta rápida».*