Los investigadores de seguridad cibernética compartieron detalles sobre una vulnerabilidad de seguridad ya parcheada en la plataforma MSHTML de Windows, que podría abusarse para eludir las protecciones de integridad en las máquinas específicas.

La vulnerabilidad, rastreada como CVE-2023-29324 (puntaje CVSS: 6.5), ha sido descrita como una omisión de función de seguridad. Microsoft lo abordó como parte de sus actualizaciones de Patch Tuesday para mayo de 2023.

El investigador de seguridad de Akamai, Ben Barnea, quien descubrió e informó el error, dijo que todas las versiones de Windows están afectadas, pero dijo que los servidores Microsoft Exchange con la actualización de marzo omiten la característica vulnerable.

> *«Un atacante no autenticado en Internet podría usar la vulnerabilidad para obligar a un cliente de Outlook a conectarse a un servidor controlado por el atacante»,* dijo Barnea en un informe.

> *«Esto da como resultado el robo de credenciales NTLM. Es una vulnerabilidad de cero clics, lo que significa que puede activarse sin interacción del usuario».*

Cabe mencionar que CVE-2023-29324 es una omisión para una solución de Microsoft implementó en marzo de 2023 para resolver CVE-2023-23397, una vulnerabilidad de escalada de privilegios en Outlook que, según la compañía, ha sido explotada por hackers rusos en ataques dirigidos a entidades europeas desde abril de 2022.

Akamai dijo que el problema se deriva del manejo complejo de las rutas en Windows, lo que permite que un hacker cree una URL maliciosa que puede eludir las comprobaciones de la zona de seguridad de Intetnet.

> *«Esta vulnerabilidad es otro ejemplo más de revisión de parches que conduce a nuevas vulnerabilidades y omisiones. Es una superficie de ataque de análisis de medios sin clic que podría contener vulnerabilidades críticas de corrupción de memoria»,* dijo Barnea.

Para mantenerse completamente protegido, Microsoft recomienda a los usuarios que instalen las actualizaciones acumulativas de Internet Explorer para abordar las vulnerabilidades en la plataforma MSHTML y el motor de secuencias de comandos.