Microsoft revisó la gravedad de una vulnerabilidad de seguridad que parcheó originalmente en septiembre de 2022 y la actualizó a *«Crítico»* después de que su equipo supo que podría explotarse para lograr la ejecución remota de código.

Rastreada como CVE-2022-37958 (puntaje CVSS: 8.1), la vulnerabilidad se describió previamente como una vulnerabilidad de divulgación de información en el mecanismo de seguridad de negociación extendida SPNEGO (NEGOEX).

SPNEGO, abreviatura de Mecanismo de Negociación GSSAPI simple y protegido, es un esquema que permite que un cliente y un servidor remoto lleguen a un consenso sobre la elección del protocolo que se usará (por ejemplo, Kerberos o NTLM) para la autenticación.

Pero un análisis más detallado de la vulnerabilidad por parte de la investigadora de IBM Security X-Force, Valentina Palmiotti, descubrió que podría permitir la ejecución remota de código arbitrario, lo que llevó a Microsoft a reclasificar su gravedad.

> *«Esta vulnerabilidad es una vulnerabilidad de ejecución remota de código previa a la autenticación que afecta a una amplia gama de protocolos. Tiene el potencial de ser gusano»,* dijo IBM esta semana.

Especialmente, la deficiencia podría permitir la ejecución remota de código por medio de cualquier protocolo de aplicación de Windows que autentique, inclyendo HTTP, SMB y RDP. Debido a la criticidad del problema, IBM dijo que retendrá los detalles técnicos hasta el segundo trimestre de 2023 para dar a las organizaciones tiempo suficiente para aplicar las correcciones.

> *«La explotación exitosa de la vulnerabilidad requiere que un atacante prepare el entorno de destino para mejorar la confiabilidad de la explotación»*, advirtió Microsoft en su aviso.

> *«A diferencia de la vulnerabilidad (CVE-2017-0144) explotada por EternalBlue y usada en los ataques de ransomware WannaCry, que solo afectó al protocolo SMB, esta vulnerabilidad tiene un alcance más amplio y podría afectar potencialmente a una gama más amplia de sistemas Windows debido a una superficie mayor de ataque a los servicios expuestos en la Internet pública (HTTP, RDP, SMB) o en redes internas»*, dijo IBM.