Microsoft recomienda a los clientes a parchear dos vulnerabilidad de seguridad en los controladores de dominio de Active Directory que abordó en noviembre, esto luego de la disponibilidad de una herramienta de prueba de concepto (PoC) publicada el 12 de diciembre.

Las dos vulnerabilidades, rastreadas como CVE-2021-42278 y CVE-2021-42287, tienen una calificación de gravedad de 7.5 y se refieren a una falla de escalada de privilegios que afecta al componente de Servicios de Dominio de Active Directory (AD DS). Andrew Barlett, de Catalyst IT, fue quien descubrió y notificó sobre ambos errores.

Active Directory es un servicio de directorio que se ejecuta en Microsoft Windows Server y se utiliza para la gestión de identidades y accesos. Aunque la compañía marcó las deficiencias como *«explotación menos probable»* en su evaluación, la divulgación pública de la PoC ha provocado nuevos llamamientos para aplicar las correcciones para mitigar cualquier posible explotación por parte de los actores de amenazas.

Mientras que CVE-2021-42278 permite a un atacante manipular el atributo SAM-Account-Name, que se utiliza para iniciar sesión a un usuario en sistemas en el dominio de Active Directory, CVE-2021-42287 permite hacerse pasar por los controladores de dominio. Esto efectivamente otorga a un atacante con credenciales de usuario de dominio acceso como usuario administrador de dominio.

> *«Al combinar estas dos vulnerabilidades, un atacante puede crear un camino sencillo para un usuario administrador de dominio en un entorno de Active Directory que no ha aplicado estas nuevas versiones. Este ataque de escalada permite a los atacantes elevar fácilmente sus privilegios a los de un administrador de dominio una vez que comprometen a un usuario normal en el dominio»,* dijo el director de producto senior de Microsoft, Daniel Naim.

La compañía también proporcionó una guía paso a paso para ayudar a los usuarios a determinar si las vulnerabilidades podrían haber sido explotadas en sus entornos. *«Como*

siempre, recomendamos encarecidamente implementar los últimos parches en los controladores de dominio lo antes posible», dijo Microsoft.