	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 093	**Fecha: 20-04-2023**
		Página 10 de 31

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los ataques que pueden tener como objetivo su Active Directory de Windows		
Tipo de ataque	Creación de usuarios sin autorización	Abreviatura	CreUsuSinAut
Medios de propagación	Red, Internet		
Código de familia	A	Código de subfamilia	A02
Clasificación temática familia	Acceso no autorizado		

Descripción

ANTECEDENTES:

El 15 de abril del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tiene conocimiento que Active Directory está en el centro de muchos ataques, ya que sigue siendo la fuente predominante de gestión de acceso e identidad en la empresa.

DETALLES:

Existen muchos ataques diferentes dirigidos a los Servicios de dominio de Active Directory (AD DS). Tenga en cuenta los siguientes ataques modernos utilizados contra AD DS.

Los controladores de dominio que alojan los servicios de dominio de Active Directory utilizan un tipo de replicación para sincronizar los cambios. Un atacante experimentado puede imitar la actividad de replicación legítima de un controlador de dominio y usar la solicitud GetNCChanges para solicitar hash de credenciales del controlador de dominio principal.

El ataque DCShadow es muy similar al ataque DCSync, ya que aprovecha el tráfico de comunicaciones legítimo de Active Directory entre los controladores de dominio. Además, el ataque DCShadow utiliza el comando DCShadow como parte del módulo Mimikatz lsadump.

Utiliza instrucciones en el protocolo remoto del servicio de replicación de directorios de Microsoft. Permite a los atacantes registrar un controlador de dominio no autorizado en el entorno y replicar los cambios en otros controladores de dominio en segundo plano. Puede incluir agregar cuentas controladas por hackers informáticos al grupo de administradores de dominio.

El rociado de contraseñas es un ataque de contraseñas dirigido a contraseñas de cuentas débiles en los servicios de dominio de Active Directory. Con el rociado de contraseñas, los atacantes usan una única contraseña común o débil y prueban esta misma contraseña en varias cuentas de Active Directory. Ofrece ventajas sobre el clásico ataque de fuerza bruta, ya que no provoca bloqueos de cuentas, ya que el atacante solo prueba la contraseña una vez por cuenta. De esta forma, los atacantes pueden encontrar contraseñas débiles en el entorno de varios usuarios.

RECOMENDACIONES:

- Implementar buenas prácticas de seguridad, protegiendo las cuentas privilegiadas con contraseñas seguras.
- Eliminar cuentas innecesarias de Active Directory, incluidas las cuentas de servicio.
- Supervisar los cambios en los grupos de dominio y otras actividades.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/security/the-attacks-that-can-target-your-windows-active-directory/