Nro. Alerta:	EC-2021-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	23-dic-2021	**Vulnerabilidades de Active Directory siguen siendo explotadas por delincuentes informáticos**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistema vulnerable / escalamiento de privilegios

Nivel de riesgo: Medio

II. ALERTA

Durante el ciclo de actualización de seguridad de noviembre, Microsoft lanzó un parche para dos nuevas vulnerabilidades, CVE-2021-42287 y CVE-2021-42278. Ambas vulnerabilidades se describen como una "vulnerabilidad de escalada de privilegios del servicio de dominio de Windows Active Directory".

III. INTRODUCCIÓN

Microsoft catalogó dos vulnerabilidades como CVE-2021-42287 y CVE-2021-42278 describiéndolas como “vulnerabilidad de escalada de privilegios del servicio de dominio de Windows Active Directory”. Estos problemas en cuestión permiten a una persona obtener fácilmente privilegios de administrador de dominio en Active Directory después de comprometer una cuenta de usuario normal. Microsoft ha publicado tres parches para su despliegue inmediato en los controladores de dominio:

- KB5008102—Active Directory Security Accounts Manager hardening changes (CVE-2021-42278)
- KB5008380—Authentication updates (CVE-2021-42287)
- KB5008602(OS Build 17763.2305) Out-of-band

IV. VECTOR DE ATAQUE

Las CVEs descritas tienen el mismo vector de ataque: a través de Red y Local

CVE-2021-42278 - Suplantación de nombre SAM, Internamente, Active Directory (AD) utiliza varios esquemas de nombres para un objeto determinado. Como userPrincipalName (UPN) y sAMAccountName (SAM-Account).

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	23-dic-2021	**Vulnerabilidades de Active Directory siguen siendo explotadas por delincuentes informáticos**	V 1.0

CVE-2021-42287 - Engaño de KDC Este CVE soluciona una vulnerabilidad que permite a un atacante potencial hacerse pasar directamente por los controladores de dominio.

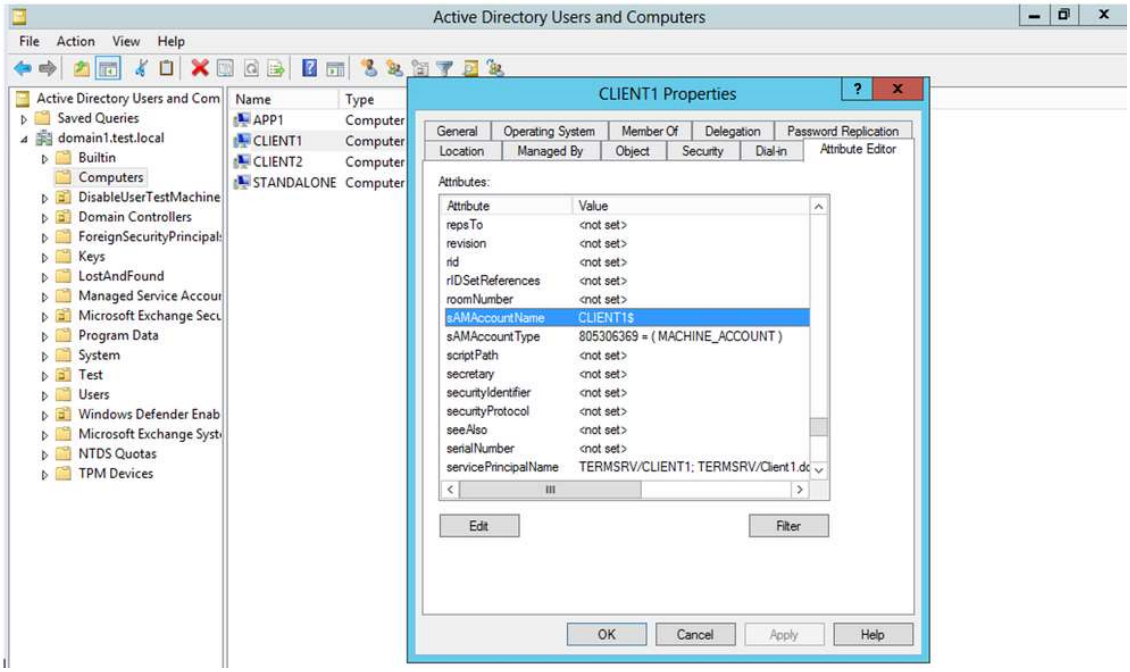

Figura 1. sAMAccountName del objeto de la computadora **Fuente:** TechCommunity Microsoft

V. IMPACTO:

Para el caso de los sistemas vulnerables, los atributos sAMAccountName generalmente terminan con "$" en su nombre. Tradicionalmente, este $ se usaba para distinguir entre objetos de usuario y objetos de computadora. Es importante mencionar que no existen restricciones ni validaciones para cambiar este atributo para incluir o no el signo $.

Con la configuración predeterminada, cuando no se aplica el parche correspondiente, un usuario normal tiene permiso para modificar la cuenta de una máquina (hasta 10 máquinas) y, como propietario, también tiene los permisos para editar su atributo sAMAccountName.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2021-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	23-dic-2021	**Vulnerabilidades de Active Directory siguen siendo explotadas por delincuentes informáticos**	V 1.0

Si hay un controlador de dominio con un nombre de cuenta SAM de DC1 $, un atacante puede crear una nueva cuenta de máquina y cambiar el nombre de su cuenta SAM a DC1, al combinar las dos CVE, un atacante con credenciales de usuario de dominio puede aprovecharlas para otorgar acceso como usuario administrador de dominio en unos pocos pasos simples.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Mantener siempre al día las actualizaciones de todos los sistemas de hardware existentes, tanto a nivel de Sistema operativo como de BIOS.
- Descargar actualizaciones, parches, hotfixes, y, siempre mantenerse al día al respecto, exclusivamente desde fuentes oficiales del fabricante.
- Crear, administrar y monitorear políticas de grupo - GPO para evitar movimientos de usuario no deseados a través de la infraestructura de red de la Institución.
- En el caso de utilizar software bajo licencia, mantener las mismas siempre al día, adquirirlas y administrarlas de forma legal únicamente.

VII. REFERENCIAS:

Daniel Naim. (20 de diciembre de 21). TechCommunity Microsoft. Obtenido de https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sam-name-impersonation/ba-p/3042699

José Palacios. (21 de diciembre de 2021). Microsofters. Obtenido de https://microsofters.com/183032/cuidado-una-vulnerabilidad-amenaza-active-directory/