BOLETÍN DE ALERTA

Boletín Nro.: 2021-40

Fecha de publicación: 22/12/2021

Tema: Microsoft publica parches para vulnerabilidades en Active Directory

Sistemas afectados:

- Windows Server 2012, 2012 R2.
- Windows Server 2008, 2008 R2.
- Windows Server 2016.
- Windows Server 20H2.
- Windows Server 2004.
- Windows Server 2022.
- Windows Server 2019.

Descripción:

Microsoft ha publicado parches de seguridad que contemplan dos vulnerabilidades denominadas CVE-2021-42287 y CVE-2021-42278, ambas de severidad alta, con una puntuación de 7.5. La falla reside en los controles de seguridad que permitirían a un atacante evadirlas para luego realizar un spoofing del *sAMAccountName* del controlador del dominio, logrando así un escalamiento de privilegios.

A continuación. se describen las vulnerabilidades:

- CVE-2021-42278: Suplantación de identidad en sAMAccountName. La falla se debe a un problema de omisión de seguridad que permite poseer un controlador de dominio al aprovechar la suplantación del atributo sAMAccountName. En particular, los mecanismos de validación de Active Directory no comprueban el carácter $ al final del nombre de la cuenta de la computadora, aunque todos los nombres de las máquinas deben terminar con él.

- CVE-2021-42287: Elevación de privilegios de los controladores de dominio de Active Directory. La vulnerabilidad se debe a una omisión de seguridad que afecta al certificado de atributo de privilegio de Kerberos (PAC). La falla se debe a la mala configuración del centro de distribución de claves (KDC) que permite que cualquier cuenta de computadora se haga pasar por dominios de Active Directory.

Debido a la publicación del PoC, los investigadores dijeron que pudieron usar fácilmente la herramienta para escalar privilegios de un usuario estándar de Active Directory a un administrador de dominio en configuraciones predeterminadas.

Impacto:

La explotación de estas vulnerabilidades en conjunto permitiría a un atacante tomar control

del dominio afectado.

Detección:

Microsoft ha compartido una guía paso a paso para detectar posibles intentos de ataques:

1. Habilitar la auditoria de los cambios del *sAMAccountName* (evento 4662) en el dominio. Como habilitarlo se encuentra en el siguiente enlace.

2. Ingresar en la opción *Advanced Haunting* en Microsoft 365 Defender. Como ingresar a la opción indicada se encuentra en el siguiente enlace.

3. Utilizar el siguiente *query* detallado a continuación. El mismo se encuentra disponible en el siguiente enlace de *GitHub*.

```
IdentityDirectoryEvents
| where Timestamp > ago(1d)
| where ActionType == "SAM Account Name changed"
| extend FROMSAM = parse_json(AdditionalFields)['FROM SAM Account Name']
| extend TOSAM = parse_json(AdditionalFields)['TO SAM Account Name']
| where (FROMSAM has "$" and TOSAM !has "$")
        or TOSAM in ("DC1", "DC2", "DC3", "DC4") // DC Names in the org
| project Timestamp, Application, ActionType, TargetDeviceName, FROMSAM, TOSA
M, ReportId, AdditionalFields
```

4. Del *query* anterior reemplazar los ejemplos ("DC1", "DC2", "DC3", "DC4") por nombres de controlador de dominio utilizado en su entorno de *Active Directory.*

5. Correr el *query* y analizar los resultados que contienen los dispositivos afectados.

6. Investigar los equipos y determinar si estos fueron comprometidos. En caso de sospecha ingresar en el siguiente enlace.

Solución:

Se recomienda actualizar el Active Directory con los parches de seguridad mediante Windows Update:

- KB5008102: https://support.microsoft.com/en-us/topic/kb5008102-active-directory-security-accounts-manager-hardening-changes-cve-2021-42278-5975b463-4c95-45e1-831a-d120004e258e

- KB5008380: https://support.microsoft.com/en-us/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041

- KB5008602: https://support.microsoft.com/en-us/topic/november-14-2021-kb5008602-os-build-17763-2305-out-of-band-8583a8a3-ebed-4829-b285-356fb5aaacd7

Información adicional:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42287
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42278
- https://nvd.nist.gov/vuln/detail/CVE-2021-42287
- https://nvd.nist.gov/vuln/detail/CVE-2021-42278
- https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-easy-windows-domain-takeover-via-active-directory-bugs/
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/sam-name-impersonation/ba-p/3042699