BOLETÍN DE ALERTA

Boletín Nro.: 2020-29

Fecha de publicación: 16/09/2020

Tema: Explotación de vulnerabilidad crítica en Netlogon Remote Protocol (MS-NRPC) "Zerologon"

Sistemas afectados:

- Windows Server 2008 R2 Service Pack 1;
- Windows Server 2008 R2 Service Pack 1 Server Core installation;
- Windows Server 2012;
- Windows Server 2012 Server Core installation;
- Windows Server 2012 R2;
- Windows Server 2012 R2 Server Core installation;
- Windows Server 2016;
- Windows Server 2016 Server Core installation;
- Windows Server 2019;
- Windows Server 2019 Server Core installation;
- Windows Server, version 1903 Server Core installation;
- Windows Server, version 1909 Server Core installation;
- Windows Server, version 2004 Server Core installation.

Descripción:

En nuestro **Boletín de Seguridad Nro.: 2020-24**, correspondiente a los **parches de Microsoft del mes de agosto**, hemos informado acerca de parches disponibles para una vulnerabilidad identificada con el **CVE-2020-1472** **de riesgo crítico**, en el **Netlogon** Remote Protocol (MS-NRPC) de Microsoft **para Windows Server**, entre otras vulnerabilidades. Sin embargo, recientemente se han publicado detalles técnicos sobre la explotación de múltiples exploits de mencionada vulnerabilidad, por lo que reiteramos el comunicado. Se trata de una vulnerabilidad de elevación de privilegios en los controladores de dominio realizada por

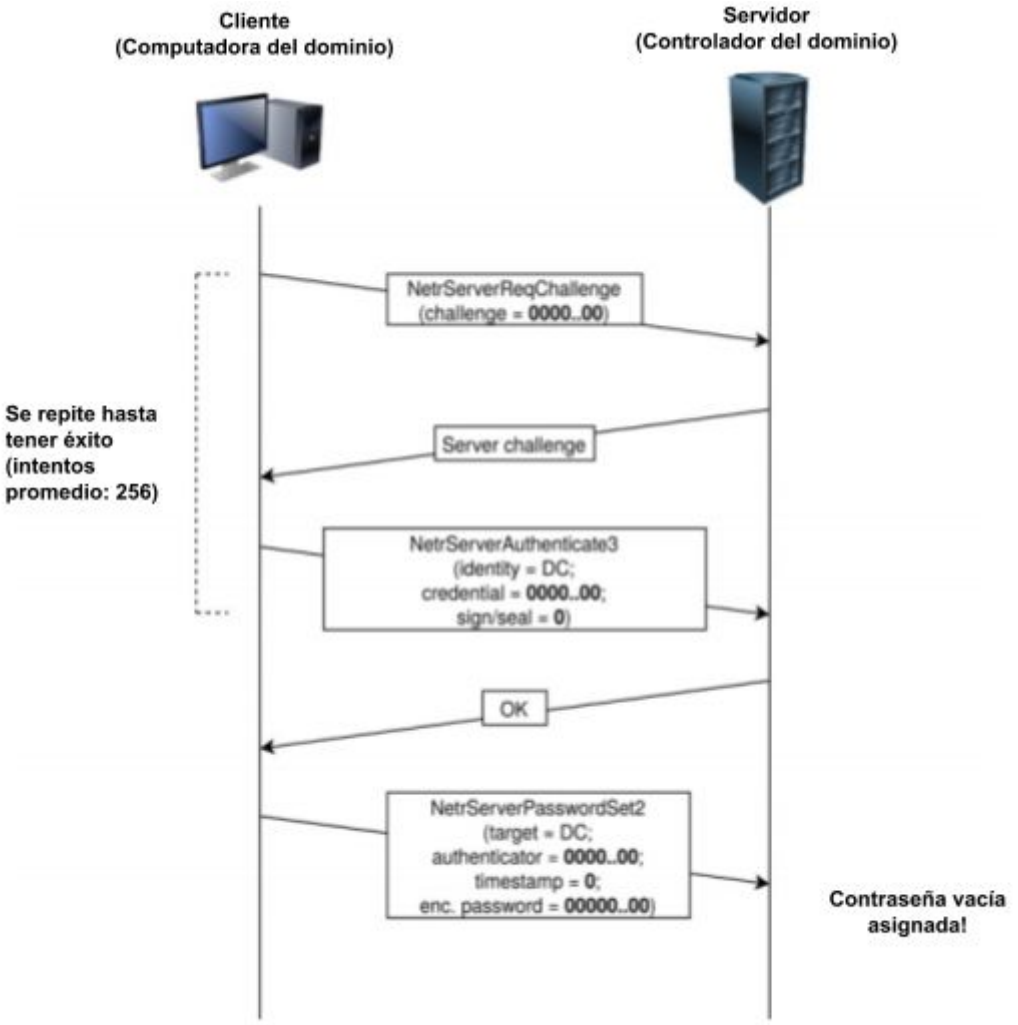
atacantes del tipo man-in-the-middle, por lo que el impacto de explotación exitosa podría causar daños importantes en los sistemas afectados.

Tal como lo informó Microsoft esta vulnerabilidad en particular, se da debido a un fallo en el esquema de autenticación criptográfico utilizado por el **Protocolo Remoto Netlogon (MS-NRPC)**, el cual es gestionado a través de una interfaz **RPC (Remote Procedure Call).**Este protocolo es utilizado generalmente para tareas relacionadas con la **autenticación de usuarios y equipos**, con el fin de facilitar a los usuarios el inicio de sesión en servidores utilizando el protocolo NTLM.

Netlogon utiliza un protocolo criptográfico personalizado que permite que un equipo cliente del dominio y el servidor o controlador de dominio certifiquen entre sí que ambos conocen un secreto compartido, el cual se trata del hash de la contraseña del equipo cliente.

La vulnerabilidad reside en el **uso del cifrado AES-CFB8** para el protocolo de autenticación inicial, y es debido a que permite una omisión de autenticación severa. Esto gracias a un cifrado débil y no aleatorio durante el procesamiento de parámetros de entrada de datos con valores cero. **Un atacante con acceso a la red podría explotar exitosamente este fallo y establecer una nueva contraseña en el controlador de dominio**, utilizar dicha contraseña obtenida para comprometer el controlador de dominio y obtener las credenciales de un usuario administrador. **Esta vulnerabilidad ha sido denominada "Zerologon" debido a la ausencia total de autenticación a la hora de realizar la explotación.**

El funcionamiento de los exploits que se aprovechan de esta vulnerabilidad, recientemente publicados, puede observarse en la siguiente imagen**:**



Impacto:

La explotación exitosa de este fallo podría permitir a un atacante:

- Manipular los procedimientos de autenticación Netlogon,
- Suplantar la identidad de cualquier equipo en la red al intentar autenticarse en el controlador de dominio,
- Obtener privilegios de administrador dominio,
- Deshabilitar las características de seguridad en el proceso de autenticación de Netlogon y

- Cambiar la contraseña de un equipo en el AD (Active Directory) del controlador del dominio.

Solución y prevención:

- Verificar la versión afectada y aplicar el parche de seguridad disponible en el sitio web oficial del fabricante en el apartado **Security Updates**, del **aviso de seguridad**.
- Seguir las instrucciones establecidas por **Microsoft** sobre cómo administrar los cambios en las conexiones de canal seguro de **Netlogon** asociadas con el **CVE-2020-1472**, disponible en el siguiente **enlace**.

Información adicional:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
- https://www.zdnet.com/article/zerologon-attack-lets-hackers-take-over-enterprise-networks/
- https://www.secura.com/blog/zero-logon
- https://www.ccn-cert.cni.es/seguridad-al-dia/alertas-ccn-cert/10477-ccn-cert-al-09-20-vulnerabilidad-zerologon.html