ACTUALIZACION BOLETIN DE CIBERSEGURIDAD

VULNERABILIDAD Zerologon (CVE-2020-1472)

Vulnerabilidades Microsoft Windows

Fecha de publicación: **11/08/2020**

Nivel de criticidad: **CRITICO**

El Centro de Operaciones de Ciberseguridad – CSOC-CERT de Gamma Ingenieros informa sobre una vulnerabilidad detectada en el Servicio de Active Directory de Windows Server. Solución que hace parte de los productos de **Microsoft.**

Antecedentes:

El 11 de septiembre, los investigadores de Secura publicaron una entrada de blog sobre una vulnerabilidad crítica que llamaron "Zerologon". La publicación del blog contiene un documento técnico que explica el impacto total y la ejecución de la vulnerabilidad, identificada como CVE-2020-1472, que recibió una puntuación CVSSv3 de 10.0, la puntuación máxima. El parche que remedia la vulnerabilidad Zerologon fue publicado por Microsoft en la ronda de actualizaciones de parches de agosto . Esta divulgación sigue a una vulnerabilidad anterior relacionada con Netlogon, CVE-2019-1424, que Secura detalló a fines del año pasado.

Existen múltiples pruebas de concepto y por eso es tan importante el parchado urgente de los sistemas afectados

CVE	PUNTUACIÓN – CRITICIDAD	TIPO VULNERABILIDAD	PRODUCTOS AFECTADOS
CVE-2020-1472	9/10 - CRITICO	Vulnerabilidad de elevación de privilegios de Netlogon	Windows Server Active Directory

A continuación, una breve descripción de la base con la cual trabaja esta vulnerabilidad detectada.

El protocolo remoto de Netlogon (también llamado MS-NRPC) es una interfaz RPC que se usa exclusivamente por dispositivos unidos a un dominio. MS-NRPC incluye un método de autenticación y un método para establecer un canal seguro de netlogon. Estas actualizaciones exigen el comportamiento específico del cliente Netlogon para usar RPC seguro con canal seguro de Netlogon entre equipos miembros y controladores de dominio (DC) de Active Directory (AD).

CVE-2020-1472: Existe una vulnerabilidad de elevación de privilegios cuando un atacante establece una conexión de canal seguro Netlogon vulnerable a un controlador de dominio, utilizando el protocolo remoto de Netlogon (MS-NRPC). Un atacante que aprovechara con éxito la vulnerabilidad podría ejecutar una aplicación especialmente diseñada en un dispositivo de la red.
Para aprovechar la vulnerabilidad, se requeriría que un atacante no autenticado usara MS-NRPC para conectarse a un controlador de dominio para obtener acceso de administrador de dominio.

Sistemas Afectados:

Windows Server 2008 R2 para sistemas basados en x64 Service Pack 1
Windows Server 2008 R2 para sistemas basados en x64 Service Pack 1 (instalación Server Core)
Windows Server 2012
Windows Server 2012 (instalación Server Core)
Windows Server 2012 R2
Windows Server 2012 R2 (instalación Server Core)
Windows Server 2016
Windows Server 2016 (instalación Server Core)
Windows Server 2019
Windows Server 2019 (instalación Server Core)
Windows Server, versión 1903 (instalación Server Core)
Windows Server, versión 1909 (instalación Server Core)
Windows Server, versión 2004 (instalación Server Core)

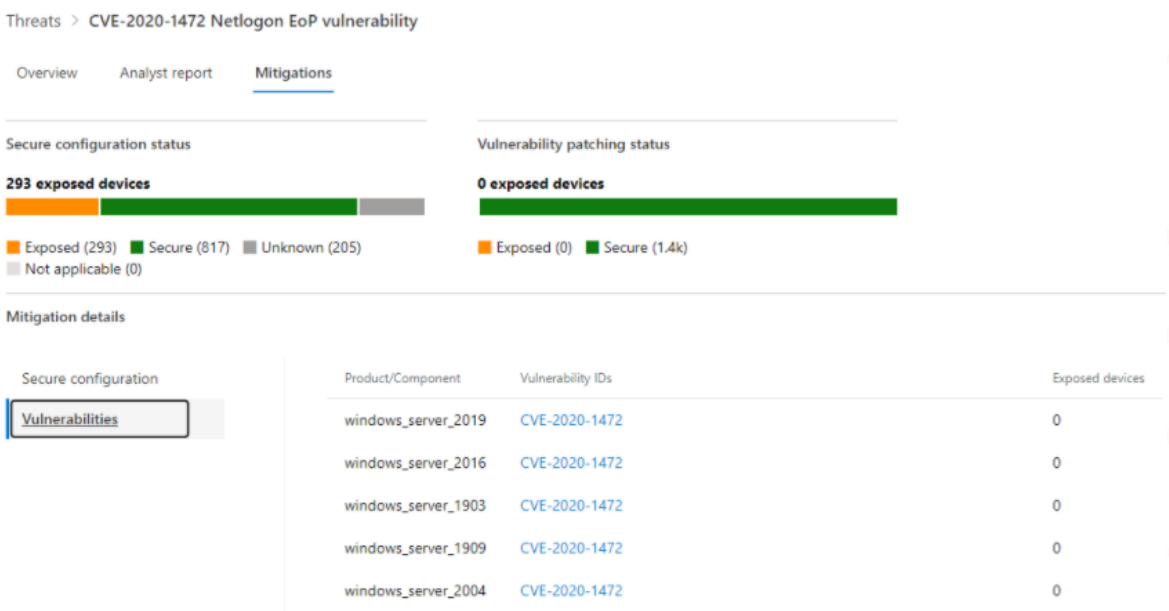
Actualización:

Casos presentados actualmente:

Microsoft asegura que está rastreando activamente la actividad de los piratas informáticos utilizando exploits para la vulnerabilidad CVE-2020-1472 Netlogon EoP, denominada Zerologon. Indican que han observado ataques en los que se han incorporado exploits públicos.

Muestran tres ejemplos que según la compañía se han estado utilizando para llevar a cabo ataques con el objetivo de explotar la vulnerabilidad Zerologon que permite, como hemos visto, obtener privilegios elevados.

Estos ejemplos son ejecutables .NET que tienen el nombre de archivo SharpZeroLogon.exe. Sin embargo, al menos por el momento, desde Microsoft no comparten más detalles sobre estos ataques.



Solución:

Por medio de las actualizaciones que libera Microsoft, las cuales se publican en dos fases: la fase inicial de las actualizaciones publicadas el 11 de agosto de 2020 y la fase de exigencia para las actualizaciones publicadas el 9 de febrero de 2021 o después.

Estas se describen con detalle sobre el siguiente enlace emitido por la entidad:

https://support.microsoft.com/es-co/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

REFERENCIAS:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472

https://www.rapid7.com/db/vulnerabilities/msft-cve-2020-1472

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472

https://support.microsoft.com/es-co/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

https://www.redeszone.net/noticias/seguridad/microsoft-alerta-ataques-zerologon/

Cordialmente,

GammaCSOC-CERT
By Gamma Ingenieros