CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad en el Estándar SAMBA

Fecha: 02/08/2022

Problemática: Vulnerabilidad en el protocolo Server Message Block SMB

Correlativo: AA-0005

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Se alerta a las instituciones gubernamentales en general sobre varias vulnerabilidades críticas en la implementación del protocolo Server Message Block SMB.

SITUACIÓN

La explotación de la vulnerabilidad en el protocolo Server Message Block - SMB podría permitir a un ciberdelincuente la ejecución arbitraria de código que puede propagarse rápidamente por redes de computadoras que utilicen una versión vulnerable del protocolo.

La capacidad de desencadenar la ejecución de código arbitrario a través de una red, le dará al atacante la capacidad de ejecutar código remoto (RCE) creando así una conexión remota hacia el sistema objetivo.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Se exhorta a realizar las acciones recomendadas por el fabricante samba.org

1. Si utiliza la versión 4.16, actualice a la versión 4.16.4
2. Si utiliza la versión 4.15, actualice a la versión 4.15.9
3. Si utiliza la versión 4.14, actualice a la versión 4.14.14

DICCIONARIO DE DATOS

1. SMB (Server Message Block): Protocolo de red que permite compartir archivos, impresoras, etc.
2. SAMBA: Conjunto estándar de programas de interoperabilidad de Windows para Linux y Unix.
3. Ejecución Arbitraria de Código: Capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
4. Ejecución de Código Remoto RCE: Es un tipo de vulnerabilidad que le otorgará al ciberdelincuente la capacidad de acceder y cambiar la propiedad de un servidor o base de datos.
5. Ciberdelincuente: Persona que se aprovecha de fallas de seguridad encontradas en plataformas, programas o sistemas a título personal

REFERENCIAS

1. Publicación código dañino Neshta https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/12012-publicado-el-nuevo-informe-de-codigo-danino-id-09-22-sobre-el-ransomware-neshta.html
2. Informe Técnico del código dañino ID-09/22 sobre el ransomware Neshta https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6690-ccn-cert-id-09-22-vice-society-neshta-1/file.html

ÁREA PARA DEFINICIONES

La información contenida en este documento y sus anexos son CONFIDENCIALES y puede contener información PRIVILEGIADA para uso exclusivo de su destinatario intencional. Si lo ha recibido por ERROR o si no es su destinatario intencional, favor NOTIFIQUELO al remitente y bórrelo inmediatamente de su sistema, así como todos los adjuntos y las COPIAS generadas. La distribución, copia u otro uso de este mensaje por terceras personas está PROHIBIDA y puede resultar ilegal.

La presente herramienta tiene aplicación práctica derivado a un proceso previo de análisis con base al contexto y la situación del evento, sin embargo, se aclara que el presente sirve como guía y marco de referencia.