

Alerta ID:	53
Fecha del reporte:	24/06/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Vulnerabilidades En Microsoft Windows Server
Herramienta de detección	N/A
Activo involucrado:	Microsoft Windows Server
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una tendencia activa de explotación de vulnerabilidades críticas en Microsoft Windows Server, incluidas aquellas catalogadas dentro del CISA Known Exploited Vulnerabilities (KEV), las cuales están siendo utilizadas en campañas reales de ataque para comprometer infraestructura crítica basada en sistemas Windows.

El propósito de esta alerta es que las entidades del sector salud validen la exposición y estado de actualización de sus servidores Windows, especialmente aquellos que soportan servicios de Active Directory, autenticación de usuarios, historia clínica electrónica (HCE), bases de datos clínicas y sistemas administrativos, con el fin de identificar posibles escenarios de compromiso



derivados de la explotación de vulnerabilidades de ejecución remota de código (RCE), escalamiento de privilegios (EoP) y fallas en servicios de red expuestos.

Esta validación debe incluir la revisión de inventarios tecnológicos de servidores Windows, controladores de dominio, servicios de virtualización, infraestructura híbrida y sistemas interconectados, con el fin de reducir el riesgo de acceso no autorizado, movimiento lateral dentro de la red hospitalaria y afectación de la continuidad operativa de los servicios de salud.

Descripción:

Se ha identificado una tendencia activa de explotación de vulnerabilidades críticas en Microsoft Windows Server, incluidas múltiples fallas catalogadas dentro del CISA Known Exploited Vulnerabilities (KEV), las cuales están siendo utilizadas en campañas reales de ataque dirigidas contra infraestructura corporativa y sectores críticos como el sector salud.

Estas vulnerabilidades incluyen principalmente fallos de tipo Remote Code Execution (RCE) y Elevation of Privilege (EoP), que afectan componentes esenciales del sistema operativo como servicios de red, autenticación, administración remota y el núcleo de Windows. En algunos casos, estas fallas han sido clasificadas como zero-days o vulnerabilidades explotadas activamente antes de la disponibilidad de un parche completo, lo que incrementa significativamente el nivel de riesgo.

Los atacantes están aprovechando principalmente servicios expuestos o mal configurados en entornos Windows Server, tales como **Active Directory, SMB, RDP, HTTP.sys e IIS**, para obtener acceso inicial a los sistemas. Una vez comprometido el servidor, los actores de amenaza pueden ejecutar código arbitrario, escalar privilegios hasta niveles administrativos y comprometer la integridad del dominio completo.



El entorno Windows Server es especialmente atractivo para los atacantes debido a su rol central en la gestión de identidades, autenticación de usuarios y administración de recursos críticos. Su compromiso permite el acceso a múltiples sistemas interconectados, facilitando el movimiento lateral dentro de la red y la expansión del ataque hacia servicios clínicos, administrativos y de almacenamiento de datos.

En el contexto del sector salud, la explotación de estas vulnerabilidades representa un riesgo elevado, ya que los servidores Windows suelen soportar sistemas de historia clínica electrónica, plataformas de laboratorio, servicios de facturación y autenticación de personal médico, lo que podría derivar en interrupciones operativas, exfiltración de información sensible y afectación directa a la continuidad de los servicios asistenciales.

Consecuencias de la explotación

La explotación exitosa de vulnerabilidades críticas en **Microsoft Windows Server**, incluidas aquellas catalogadas dentro del **CISA KEV** y tendencias de zero-days en explotación activa, puede generar impactos severos tanto a nivel técnico como operativo en las organizaciones del sector salud.

1. Compromiso total del servidor (RCE / EoP)

Los atacantes pueden ejecutar código arbitrario o escalar privilegios dentro del sistema operativo Windows Server, obteniendo control total del servidor comprometido.

Esto permite la manipulación de servicios críticos, la instalación de malware y la desactivación de mecanismos de seguridad.



2. Compromiso del dominio (Active Directory)

Dado el rol central de Windows Server como controlador de dominio, su explotación puede derivar en la toma completa del entorno de autenticación.

Esto permite:

- Control total de usuarios y permisos
- Creación de cuentas administrativas ocultas
- Acceso a todos los sistemas conectados al dominio

3. Movimiento lateral en infraestructura hospitalaria

Una vez comprometido el servidor, los atacantes pueden propagarse hacia otros sistemas críticos del entorno de salud, incluyendo:

- Historia clínica electrónica (HCE)
- Sistemas de laboratorio clínico
- Servidores de imágenes diagnósticas (PACS)
- Plataformas administrativas y financieras

4. Ejecución de ataques de ransomware

Windows Server es un objetivo frecuente en cadenas de ransomware, donde su compromiso permite:

- Cifrado masivo de información crítica
- Eliminación de copias de seguridad
- Interrupción de servicios hospitalarios esenciales



5. Exfiltración de información sensible

El acceso privilegiado al servidor permite la extracción de:

- Datos clínicos de pacientes
- Credenciales institucionales
- Información administrativa y financiera
- Registros de auditoría y seguridad

6. Interrupción de servicios críticos de salud

La explotación puede afectar directamente la disponibilidad de sistemas esenciales, generando:

- Caída de autenticación de usuarios (AD)
- Indisponibilidad de aplicaciones clínicas
- Interrupción de sistemas de atención médica digital
- Fallas en servicios interconectados entre sedes

7. Impacto regulatorio y reputacional

El compromiso de información sensible puede derivar en:

- Incumplimiento de la Ley 1581 de 2012 (Colombia)
- Sanciones regulatorias por fuga de datos personales
- Afectación de la confianza institucional



- Daño reputacional en el sector salud

8. Persistencia del atacante

El control de Windows Server permite a los atacantes mantener persistencia mediante:

- Creación de cuentas privilegiadas
- Manipulación de políticas de seguridad
- Instalación de herramientas de acceso remoto
- Alteración de logs y auditorías.

Modo de explotación del ataque

La explotación de vulnerabilidades críticas en **Microsoft Windows Server**, incluidas aquellas catalogadas dentro del **CISA KEV** y tendencias de zero-days en explotación activa, sigue una cadena de ataque estructurada que combina el abuso de servicios expuestos, explotación de fallos de seguridad y escalamiento de privilegios dentro de entornos corporativos:

Fase 1 – Reconocimiento de infraestructura Windows expuesta

Los actores de amenaza realizan escaneos masivos en Internet y redes internas para identificar:

- Servidores Windows expuestos (RDP, SMB, HTTP.sys, IIS)
- Controladores de dominio (Active Directory)
- Servicios de autenticación accesibles
- Interfaces de administración mal protegidas

Objetivo: identificar objetivos con versiones vulnerables o servicios expuestos.



Fase 2 – Acceso inicial al sistema (Initial Access)

El atacante obtiene acceso mediante:

- Explotación de vulnerabilidades RCE en servicios Windows
- Uso de credenciales comprometidas (phishing o leaks)
- Acceso a RDP sin MFA o protección adecuada
- Abuso de servicios expuestos (SMB / WinRM / IIS)

MITRE ATT&CK: T1190 – Exploit Public-Facing Application / T1078 – Valid Accounts

Fase 3 – Ejecución de código en el servidor (Execution)

Una vez dentro del sistema, el atacante ejecuta código arbitrario en el contexto del usuario comprometido o del servicio afectado.

Esto permite:

- Ejecución de comandos remotos
- Descarga de herramientas adicionales
- Despliegue de malware o loaders

MITRE ATT&CK: T1059 – Command and Scripting Interpreter

Fase 4 – Escalamiento de privilegios (Privilege Escalation)

El atacante explota vulnerabilidades del kernel o servicios del sistema para elevar privilegios hasta:

- SYSTEM



- Administrador de dominio (en escenarios AD comprometidos)

MITRE ATT&CK: T1068 – Exploitation for Privilege Escalation

Fase 5 – Compromiso del dominio (Active Directory)

En entornos corporativos y hospitalarios, el atacante puede comprometer Active Directory mediante:

- Kerberoasting
- Pass-the-Hash / Pass-the-Ticket
- Dumping de credenciales del controlador de dominio

Resultado: control total del entorno de autenticación.

Fase 6 – Movimiento lateral dentro de la red

Con acceso privilegiado, el atacante se desplaza hacia otros sistemas internos:

- Servidores clínicos (HCE)
- Bases de datos de pacientes
- Sistemas de laboratorio
- Infraestructura de virtualización

MITRE ATT&CK: T1021 – Remote Services

Fase 7 – Persistencia en el entorno comprometido

El atacante establece mecanismos de persistencia mediante:

- Creación de usuarios administrativos ocultos



- Modificación de políticas de grupo (GPO)
- Instalación de servicios o tareas programadas maliciosas
- Backdoors en el sistema operativo

MITRE ATT&CK: T1547 – Boot or Logon Autostart Execution

Fase 8 – Impacto final (Ransomware / Exfiltración)

En la fase final del ataque, se ejecutan acciones como:

- Cifrado masivo de información (ransomware)
- Eliminación de copias de seguridad
- Exfiltración de datos sensibles del sector salud
- Interrupción de servicios críticos hospitalarios

MITRE ATT&CK: T1486 – Data Encrypted for Impact / T1041 – Exfiltration

Vulnerabilidades asociadas

La campaña activa contra Windows Server se apoya en una combinación de vulnerabilidades críticas registradas en el catálogo **CISA KEV**, técnicas de explotación activas en entornos reales y debilidades comunes de configuración en infraestructuras corporativas, especialmente en sectores como salud.

1. Vulnerabilidades de ejecución remota de código (RCE) en servicios Windows

MITRE ATT&CK: T1190 – Exploit Public-Facing Application



Descripción

Explotación de servicios expuestos como:

- IIS (Internet Information Services)
- HTTP.sys
- SMB (Server Message Block)
- WinRM (Windows Remote Management)

Debilidades asociadas

- Servicios expuestos directamente a Internet
- Falta de segmentación perimetral
- Ausencia de filtros de acceso por IP

Impacto: ejecución remota de código sin autenticación en algunos escenarios.

2. Vulnerabilidades de escalamiento de privilegios en Windows Kernel

MITRE ATT&CK: T1068 – Exploitation for Privilege Escalation

Descripción

Fallos en el kernel permiten que un atacante pase de usuario estándar a:

- SYSTEM
- Administrador local
- Administrador de dominio (en escenarios AD comprometidos)

Debilidades asociadas



- Sistemas sin parches acumulativos recientes
- Privilegios locales mal asignados
- Usuarios con permisos administrativos innecesarios

3. Compromiso de Active Directory (AD)

MITRE ATT&CK: T1558 / T1003 / T1078

Descripción

Ataques dirigidos al sistema de autenticación central:

- Kerberoasting
- Pass-the-Hash
- Dumping de credenciales LSASS

Debilidades asociadas

- Contraseñas débiles o reutilizadas
- Ausencia de mfa en cuentas privilegiadas
- Delegación insegura en ad
- Falta de hardening en controladores de dominio

Impacto: control total del dominio corporativo.

4. Exposición de servicios de acceso remoto

MITRE ATT&CK: T1133 – External Remote Services

Descripción

Servicios expuestos comúnmente:



- RDP (Remote Desktop Protocol)
- VPN corporativa
- WinRM

Debilidades asociadas

- RDP expuesto sin MFA
- VPN sin filtrado geográfico
- Falta de restricción por IP confiables
- Ausencia de bastion hosts

5. Fallas en configuración de autenticación y credenciales

MITRE ATT&CK: T1078 – Valid Accounts

Descripción

Uso de credenciales válidas comprometidas para acceso inicial.

Debilidades asociadas

- Reutilización de contraseñas en múltiples sistemas
- Falta de rotación de credenciales administrativas
- Ausencia de monitoreo de credenciales filtradas (dark web leaks)

6. Debilidades en monitoreo y detección

MITRE ATT&CK: T1047 / T1059 / T1071

Descripción

Actividad maliciosa no detectada por:



- SIEM mal configurado o sin correlación
- Ausencia de logs centralizados
- Falta de alertas de comportamiento anómalo

Debilidades asociadas

- Logging incompleto en servidores Windows
- Falta de auditoría de Active Directory
- Ausencia de UEBA (User Behavior Analytics)

7. Falta de hardening en Windows Server

Debilidad operacional crítica

Descripción**Configuraciones inseguras frecuentes:**

- Servicios innecesarios habilitados
- Firewall de windows desactivado o mal configurado
- Políticas de grupo débiles
- Ausencia de baseline de seguridad cis/microsoft

El riesgo en Windows Server no depende de una única vulnerabilidad, sino de un ecosistema de fallas técnicas y de configuración, donde la exposición de servicios, la debilidad en la autenticación y la falta de monitoreo permiten la explotación en cadena hasta el compromiso total del dominio.

Recomendaciones de detección y mitigación

Para reducir el riesgo asociado a la explotación de vulnerabilidades críticas en **Microsoft Windows Server (incluidas aquellas en CISA KEV y tendencias de zero-days en explotación activa)**, se recomienda implementar controles de detección avanzada, correlación de eventos y fortalecimiento de la infraestructura crítica.

1. DETECCIÓN EN SOC / SIEM

1.1 Detección de ejecución de exploits y comportamiento anómalo

Configurar alertas para identificar:

- Elevación repentina de privilegios (usuario → SYSTEM)
- Ejecución de procesos inusuales desde servicios del sistema
- Uso anómalo de PowerShell o CMD en servidores críticos
- Creación de cuentas administrativas no autorizadas

1.2 Detección de explotación de Active Directory

Monitorear eventos como:

- intentos de Kerberoasting
- múltiples autenticaciones fallidas seguidas de éxito
- consultas masivas a LDAP
- acceso a LSASS o dumping de credenciales

Eventos Windows relevantes:

- 4624 (login exitoso)
- 4625 (login fallido)
- 4672 (privilegios especiales asignados)



- 4688 (creación de procesos)

1.3 Detección de movimiento lateral

Alertar sobre:

- Accesos a múltiples servidores en corto tiempo
- Uso de smb / rdp entre servidores internos
- Autenticaciones desde cuentas privilegiadas fuera de horario

1.4 Detección de cambios críticos en el sistema

Monitorear:

- Modificación de GPO (Group Policy Objects)
- Cambios en cuentas de administrador
- Desactivación de antivirus o Defender
- Alteración de reglas de firewall local

2. REGLAS DE CORRELACIÓN EN SIEM

Reglas recomendadas:

- LOGIN ADMIN + CREACIÓN DE USUARIO + MENOS DE 10 MIN → CRÍTICO
- FALLAS DE LOGIN MASIVAS + LOGIN EXITOSO → ALTO
- ACCESO A LSASS + PROCESO POWERSHELL → CRÍTICO
- RDP + MOVIMIENTO LATERAL + SMB → CRÍTICO

Fuentes de logs a centralizar:

- Windows Security Logs
- Event Viewer (System / Application)



- Active Directory logs
- Sysmon (eventos de procesos y red)
- Logs de firewall interno

3. THREAT HUNTING (BÚSQUEDA PROACTIVA)

Buscar patrones como:

- Ejecución de herramientas de dumping (Mimikatz-like behavior)
- Conexiones SMB inusuales entre servidores
- Cuentas administrativas usadas en múltiples hosts
- Powershell con parámetros ofuscados
- Tráfico interno hacia puertos administrativos (3389, 445, 5985)

4. HARDENING DE WINDOWS SERVER

4.1 Gestión de parches

- Aplicar inmediatamente actualizaciones del catálogo Microsoft Security Update
- Priorizar vulnerabilidades listadas en CISA KEV
- Implementar ciclo de parcheo mensual + emergencia (out-of-band)

4.2 Control de acceso y privilegios

- Implementar principio de mínimo privilegio
- Eliminar cuentas locales innecesarias
- Separar cuentas administrativas de usuarios estándar
- Restringir acceso a Domain Admins

4.3 Seguridad de autenticación

- Implementar MFA en accesos administrativos



- Bloquear autenticación RDP sin MFA
- Políticas de contraseñas robustas y rotación periódica

4.4 Reducción de superficie de ataque

- Deshabilitar servicios no utilizados (SMBv1, WinRM si no es necesario)
- Cerrar puertos administrativos expuestos
- Restringir RDP a redes internas o VPN segura

4.5 Segmentación de red

Separar claramente:

- servidores de dominio (AD)
- servidores clínicos (HCE)
- servidores administrativos
- red de usuarios finales

4.6 Endurecimiento del sistema operativo

- Activar Windows Defender Credential Guard
- Habilitar LSA Protection
- Activar logging avanzado (Sysmon)
- Configurar baselines CIS Microsoft Security

5. RESPUESTA AUTOMATIZADA (SOAR)

Implementar automatización para:

- Bloqueo automático de cuentas tras comportamiento sospechoso



- Aislamiento de servidores comprometidos
- Alertas en tiempo real al soc
- Creación automática de incidentes en siem

La protección de Windows Server en entornos de salud depende de una estrategia de defensa en profundidad basada en **visibilidad, control de identidad y respuesta automatizada**, ya que su compromiso implica la pérdida total del control del entorno clínico y administrativo.

Recomendaciones de prevención y mitigación

Para reducir el riesgo asociado a la explotación de vulnerabilidades críticas en **Microsoft Windows Server**, incluidas aquellas activamente explotadas y catalogadas en **CISA KEV**, se recomienda implementar un enfoque integral basado en la protección del sistema operativo, la gestión de identidad, la reducción de superficie de ataque y el monitoreo continuo:

1. 1. Gestión de parches y actualización de seguridad

- Aplicar de forma inmediata los parches de seguridad publicados por Microsoft.
- Priorizar vulnerabilidades incluidas en el catálogo CISA KEV como críticas.
- Establecer un ciclo formal de actualización:
 - Crítico: inmediato
 - Alto: máximo 72 horas – 7 días
 - Medio/Bajo: ciclo mensual
- Verificar versiones de Windows Server en todos los entornos (on-premise, nube e híbrido).

2. Fortalecimiento de Active Directory

- Aplicar hardening a controladores de dominio (Domain Controllers).



- Restringir estrictamente el uso de cuentas privilegiadas (Domain Admin).
- Eliminar cuentas inactivas o sin uso.
- Activar auditoría avanzada de cambios en AD.
- Proteger el acceso a LDAP, Kerberos y NTLM con políticas seguras.

3. Gestión de identidades y accesos (IAM)

- **Implementar autenticación multifactor (MFA) en:**
 - accesos administrativos
 - RDP
 - VPN corporativa
- Aplicar principio de mínimo privilegio.
- Separar cuentas administrativas y de usuario.
- Implementar bloqueo por intentos fallidos de autenticación.

4. Reducción de superficie de ataque

- Deshabilitar servicios no utilizados (SMBv1, WinRM si no es necesario).
- Restringir RDP a redes internas o VPN segura.
- Bloquear exposición directa de servicios críticos a Internet.
- Cerrar puertos administrativos desde redes no confiables.

5. Hardening del sistema operativo

- Activar Windows Defender Credential Guard.
- Habilitar LSA Protection.
- Aplicar políticas de seguridad basadas en CIS Benchmarks.
- Activar logging avanzado (Sysmon y Event Forwarding).



- Deshabilitar servicios y roles innecesarios.

6. Segmentación de red

- Separar claramente:
 - servidores de dominio (AD)
 - servidores clínicos (HCE / laboratorio)
 - servidores administrativos
 - red de usuarios finales
- Implementar microsegmentación para limitar movimiento lateral.

7. Monitoreo continuo y detección

- Centralizar logs en SIEM corporativo.
- Monitorear:
 - escalamiento de privilegios
 - creación de usuarios administrativos
 - autenticaciones anómalas
 - conexiones RDP/SMB inusuales
- Implementar análisis de comportamiento (UEBA).

8. Gestión de vulnerabilidades

- Realizar escaneo periódico de infraestructura Windows Server.
- Integrar inteligencia de amenazas (CISA KEV + Microsoft Security Advisories).
- Priorizar vulnerabilidades activamente explotadas.
- Validar exposición de servicios críticos en Internet.

9. Respaldo y continuidad operativa



- Mantener copias de seguridad offline e inmutables.
- Probar restauración periódica de backups.
- Proteger backups contra acceso desde dominio comprometido.

10. Concienciación y buenas prácticas

- Capacitar administradores en hardening de Windows Server.
- Promover uso seguro de credenciales.
- Fomentar reporte temprano de incidentes.

La seguridad de Windows Server en entornos críticos como el sector salud depende de una estrategia de **defensa en profundidad**, donde la combinación de gestión de parches, control de identidad y monitoreo continuo es esencial para prevenir la explotación de vulnerabilidades activamente utilizadas en campañas reales de ataque.

Recomendaciones de respuesta ante compromiso

En caso de sospecha o confirmación de compromiso en servidores **Microsoft Windows Server**, especialmente aquellos expuestos a vulnerabilidades activamente explotadas (CISA KEV), se debe activar de inmediato el procedimiento de respuesta a incidentes para contener, erradicar y recuperar la operación de forma segura:

1. Contención inmediata del incidente

- Aislar el servidor comprometido de la red (segmentación lógica o desconexión física).
- Suspender accesos remotos (RDP, VPN, WinRM) temporalmente.
- Bloquear direcciones IP asociadas a actividad sospechosa en firewall perimetral.



- Deshabilitar cuentas administrativas potencialmente comprometidas.
- Evitar reinicio inmediato si no es estrictamente necesario (preservación forense).

Objetivo: detener propagación lateral y pérdida de evidencia.

2. Preservación de evidencia digital

- Capturar memoria RAM del servidor afectado (si es posible).
- Exportar logs críticos:
 - Security Event Logs
 - System Logs
 - Active Directory logs
- Preservar configuración del sistema y reglas de firewall locales.
- Recolectar evidencia de conexiones de red (NetFlow / firewall logs).

Objetivo: permitir análisis forense posterior del ataque.

3. Análisis y validación del compromiso

- Identificar cuentas utilizadas en accesos no autorizados.
- Revisar eventos de escalamiento de privilegios (SYSTEM / Domain Admin).
- Detectar creación de cuentas ocultas o privilegios elevados.
- Analizar actividad en Active Directory (LDAP/Kerberos anómalo).



- Verificar ejecución de procesos sospechosos (PowerShell, CMD, wmic).

MITRE ATT&CK relacionado:

- T1078 – Valid Accounts
- T1068 – Privilege Escalation
- T1059 – Command Execution

4. Erradicación de la amenaza

- Revocar todas las credenciales comprometidas o sospechosas.
- Forzar cambio de contraseñas en cuentas administrativas.
- Eliminar cuentas no autorizadas creadas durante el incidente.
- Remover persistencia (tareas programadas, servicios, GPO maliciosas).
- Aplicar parches de seguridad correspondientes a vulnerabilidades KEV explotadas.

Objetivo: eliminar completamente la presencia del atacante.

5. Recuperación del entorno

- Restaurar servicios desde backups limpios e inmutables.
- Validar integridad de Active Directory antes de reintegrar servidores.
- Reincorporar el servidor a la red solo tras validación de seguridad.
- Monitorear actividad post-restauración de forma intensiva.



- Confirmar funcionamiento de sistemas críticos (HCE, laboratorio, AD).

Objetivo: restablecer operación segura del entorno hospitalario.

6. Análisis de impacto

- Determinar alcance del compromiso:
- servidores afectados
- cuentas comprometidas
- sistemas clínicos impactados
- Identificar posible exfiltración de información sensible.
- Evaluar impacto en servicios críticos de salud.

Objetivo: definir nivel de severidad del incidente.

7. Notificación y escalamiento

- Notificar al equipo SOC / CSIRT interno inmediatamente.
- Informar a líderes de TI e infraestructura.
- Escalar a entidades externas si aplica:
- CSIRT nacional
- autoridades regulatorias (SIC en Colombia si hay datos personales)
- Documentar línea de tiempo del incidente.



Objetivo: asegurar cumplimiento normativo y coordinación.

8. Lecciones aprendidas y mejora continua

- Realizar post-mortem del incidente.
- Ajustar reglas SIEM basadas en comportamiento detectado.
- Fortalecer controles de acceso (MFA, PAM, segmentación).
- Actualizar hardening de Windows Server.
- Revisar exposición de servicios en Internet.

Objetivo: evitar recurrencia del ataque.

El compromiso de un servidor Windows en entornos de salud debe considerarse un incidente de **alta criticidad**, debido a su potencial de propagación hacia Active Directory y sistemas clínicos, por lo que la respuesta debe ser rápida, coordinada y basada en evidencia forense para evitar impacto sistémico.

Conclusiones

La presente alerta evidencia una tendencia activa y sostenida de explotación de vulnerabilidades críticas en **Microsoft Windows Server**, incluidas aquellas catalogadas dentro del **CISA Known Exploited Vulnerabilities (KEV)**, las cuales están siendo utilizadas en campañas reales de ataque dirigidas a infraestructura corporativa y sectores altamente sensibles como el sector salud.



Estas vulnerabilidades, principalmente asociadas a fallos de **ejecución remota de código (RCE)**, **escalamiento de privilegios (EoP)** y compromiso de servicios críticos del sistema operativo, representan un riesgo significativo debido al rol central que Windows Server desempeña en la autenticación, gestión de identidades y operación de servicios clínicos y administrativos.

El análisis de la amenaza permite concluir que el impacto no se limita al servidor comprometido, sino que puede escalar hacia el **compromiso completo del dominio (Active Directory)**, facilitando el movimiento lateral hacia sistemas críticos como historia clínica electrónica, plataformas de laboratorio, sistemas de imágenes diagnósticas y servicios financieros del sector salud.

Adicionalmente, la explotación de estas vulnerabilidades se ve favorecida por factores estructurales como la exposición de servicios remotos (RDP, SMB, WinRM), la ausencia de autenticación multifactor en accesos privilegiados, la falta de segmentación de red y configuraciones de seguridad insuficientes en entornos Windows Server.

En este contexto, el riesgo se incrementa debido a la alta dependencia operativa de estos sistemas dentro de las organizaciones de salud, lo que puede derivar en interrupciones de servicios esenciales, pérdida de disponibilidad de sistemas clínicos, exfiltración de información sensible y afectación directa a la continuidad de la atención médica.

Se concluye que la mitigación efectiva de esta amenaza no depende únicamente de la aplicación de parches de seguridad, sino de la implementación de una estrategia integral de ciberseguridad basada en **gestión de vulnerabilidades, control de identidades, segmentación de red, monitoreo continuo y respuesta oportuna ante incidentes**.



Finalmente, se recomienda a las organizaciones del sector salud mantener un enfoque de **defensa en profundidad**, priorizando vulnerabilidades incluidas en el catálogo CISA KEV y fortaleciendo sus capacidades de detección y respuesta para reducir el riesgo de compromiso de su infraestructura crítica.

Fuentes:



- Microsoft Security Response Center (MSRC) – Publicaciones oficiales de Microsoft sobre vulnerabilidades en Windows Server, actualizaciones de seguridad y correcciones críticas de sistema operativo.
o <https://msrc.microsoft.com/update-guide>
- Microsoft Security Advisories – Documentación técnica sobre vulnerabilidades en servicios de Windows Server, Active Directory, RDP, SMB e IIS, incluyendo recomendaciones de mitigación y hardening.
o <https://www.microsoft.com/en-us/security>
- CISA Known Exploited Vulnerabilities (KEV) Catalog – Lista oficial de vulnerabilidades confirmadas como explotadas activamente en entornos reales, priorizadas para mitigación inmediata.
o <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- CISA Cybersecurity Advisories – Alertas sobre campañas activas de explotación contra infraestructura crítica, incluyendo entornos Windows Server y Active Directory.
o <https://www.cisa.gov/news-events/cybersecurity-advisories>



- MITRE ATT&CK Framework – Base de conocimiento de técnicas de ataque utilizadas en compromisos de Windows Server, Active Directory y movimiento lateral en redes corporativas.

- o <https://attack.mitre.org/>

- NIST Cybersecurity Framework – Referencia internacional para gestión de riesgos, control de acceso, protección de sistemas y respuesta a incidentes en infraestructura crítica.

- o <https://www.nist.gov/cyberframework>

- ENISA Threat Landscape – Reportes de inteligencia sobre amenazas globales dirigidas a infraestructura crítica, incluyendo servidores Windows y entornos empresariales.

- o <https://www.enisa.europa.eu/publications>

- Microsoft Security Update Guide (Windows Server) – Base de datos oficial de parches y vulnerabilidades corregidas en Windows Server y componentes asociados.

- o <https://msrc.microsoft.com/update-guide>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

