Boletín informativo
“Vulnerabilidad “Microsoft Defender.

CSIRTSALUD-AV-20260526-49 **TLP: CLEAR**

Alerta ID:	049
Fecha del reporte:	26/05/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Microsoft Defender, elevación de privilegios local
Herramienta de detección	N/A
Activo involucrado:	Microsoft Defender
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a todas las entidades del ecosistema digital sobre la reciente vulnerabilidad crítica identificada como CVE-2026-41091 en Microsoft Defender, un zero-day que permite la elevación de privilegios local. Esta alerta busca que las organizaciones revisen sus sistemas, evalúen los riesgos asociados y ejecuten acciones preventivas inmediatas para proteger endpoints y datos sensibles, especialmente en entornos corporativos y del sector salud.

Descripción:

CVE-2026-41091 es una vulnerabilidad zero-day crítica en Microsoft Defender que permite la elevación de privilegios local en sistemas Windows. Esta falla puede ser explotada por un atacante con acceso limitado al sistema para obtener permisos administrativos, permitiendo ejecutar código arbitrario con privilegios elevados. La vulnerabilidad se encuentra en la forma

en que Microsoft Defender procesa ciertas operaciones internas, lo que permite al atacante manipular objetos del sistema y evadir controles de seguridad estándar. La explotación exitosa de esta vulnerabilidad puede comprometer la integridad del endpoint, exponer datos sensibles, interferir con la protección antivirus y permitir movimientos laterales dentro de la red corporativa.

Los atacantes podrían aprovechar esta vulnerabilidad para:

- Ejecutar comandos con privilegios elevados sin autorización.
- Deshabilitar o manipular componentes de seguridad de Microsoft Defender.
- Instalar malware adicional o establecer persistencia en el sistema comprometido.
- Escalar privilegios y acceder a datos sensibles, incluyendo información personal y datos clínicos en entornos del sector salud.

Dada la naturaleza zero-day de esta vulnerabilidad, se considera de alto riesgo y requiere medidas de mitigación inmediatas, incluyendo la aplicación de parches oficiales tan pronto estén disponibles y la implementación de controles complementarios de detección y monitoreo de endpoints.

Consecuencias de la explotación

- La explotación exitosa de la vulnerabilidad CVE-2026-41091 en Microsoft Defender puede derivar en impactos significativos tanto a nivel técnico como operativo. Entre las principales consecuencias se incluyen:
- **Compromiso total del endpoint:** El atacante obtiene control completo sobre el sistema afectado, con capacidad de ejecutar comandos arbitrarios, manipular procesos críticos y acceder a recursos restringidos.

- **Evasión de controles de seguridad:** Al aprovechar fallas internas de Microsoft Defender, los atacantes pueden evadir detección y prevención de malware, retrasando la respuesta del equipo de seguridad y aumentando el tiempo de exposición (dwell time).
- **Escalamiento de privilegios:** La vulnerabilidad permite al atacante elevar sus permisos a nivel administrador, posibilitando la instalación de malware adicional, modificación de configuraciones críticas y persistencia prolongada.
- **Acceso a información sensible:** La explotación puede conducir a la exposición de datos confidenciales, incluyendo información personal, credenciales de usuarios y datos clínicos, con potencial impacto en la privacidad de pacientes y cumplimiento normativo.
- **Movimiento lateral:** Con privilegios elevados, los atacantes podrían propagarse dentro de la red corporativa, comprometiendo otros sistemas y servicios críticos.
- **Impacto operativo y reputacional:** La manipulación o desactivación de servicios de seguridad puede causar interrupciones en operaciones esenciales y afectar la confianza de los usuarios y clientes, especialmente en el sector salud.
- Estas consecuencias destacan la criticidad de aplicar medidas de mitigación inmediatas, mantener actualizado el software y fortalecer los controles de seguridad en endpoints y redes corporativas.

Modo de explotación del ataque

La vulnerabilidad CVE-2026-41091 en Microsoft Defender es explotada a nivel local por un atacante con acceso limitado al sistema. El modo de explotación se describe en varias fases:

Fase 1 – Preparación del ataque:

- El atacante obtiene acceso a un usuario estándar o cuenta con permisos limitados en el endpoint.

- Se identifican los componentes internos de Microsoft Defender que pueden ser manipulados para elevar privilegios.

Fase 2 – Ejecución del exploit:

- Se ejecuta un código especialmente diseñado que aprovecha la falla en el manejo de operaciones internas de Defender.
- Esta ejecución permite al atacante ejecutar instrucciones con privilegios de administrador, alterando procesos críticos y el control de seguridad del endpoint.

Fase 3 – Escalamiento de privilegios:

- El exploit eleva los permisos del atacante a nivel de administrador local (Local Administrator) o SYSTEM.
- Se habilita la posibilidad de instalar malware adicional, manipular configuraciones del sistema y establecer persistencia en el endpoint.

Fase 4 – Acceso y manipulación del sistema:

- Con privilegios elevados, el atacante puede:
  - Ejecutar comandos arbitrarios.
  - Deshabilitar o manipular componentes de seguridad, incluyendo protección en tiempo real y actualizaciones de Defender.
  - Acceder a datos sensibles y críticos del sistema.

Fase 5 – Propagación y movimiento lateral:

- La explotación puede ser usada como punto de pivot dentro de la red corporativa, permitiendo el compromiso de otros sistemas conectados y el acceso a información sensible adicional.

Observaciones adicionales:

Esta vulnerabilidad es considerada crítica y de alto riesgo debido a su capacidad de evadir la detección de seguridad y comprometer la integridad de los sistemas locales y corporativos.

Vulnerabilidades asociadas

Aunque CVE-2026-41091 es un zero-day específico de Microsoft Defender, su explotación se basa en varias técnicas y vectores que reflejan vulnerabilidades y configuraciones críticas del sistema:

1. **Elevación de privilegios local:** Aprovecha fallas internas en el manejo de operaciones del software de seguridad para obtener permisos de administrador o SYSTEM.
2. **Manipulación de objetos internos del sistema:** Explotación de cómo Defender procesa ciertos objetos y eventos, permitiendo ejecutar código arbitrario con privilegios elevados.
3. **Evasión de controles de seguridad:** La técnica permite eludir la protección en tiempo real y las reglas de detección basadas en firmas, exponiendo la necesidad de controles conductuales.
4. **Persistencia local:** El atacante puede modificar configuraciones del endpoint para mantener acceso elevado tras reinicios.
5. **Movimiento lateral potencial:** Con privilegios elevados, los atacantes pueden pivotar hacia otros sistemas dentro de la red corporativa:

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Privilege Escalation	T1068	Explotación de vulnerabilidad de Microsoft Defender para elevar privilegios localmente.
Defense Evasion	T1070 / T1497	Evasión de controles de seguridad de Defender y técnicas anti-análisis para evitar detección.
Persistence	T1053	Modificación de configuraciones locales para mantener acceso y control del endpoint.
Lateral Movement	T1021	Posible movimiento lateral en la red corporativa con privilegios escalados.

Táctica	Técnica / ID	Descripción en el contexto de SpankRAT
Execution	T1059	Ejecución de código arbitrario aprovechando la falla en el manejo de objetos internos del sistema.

Recomendaciones de detección y mitigación

Los equipos de seguridad, infraestructura y soporte técnico deben priorizar la validación y mitigación de la vulnerabilidad CVE-2026-41091 en Microsoft Defender, debido a que permite elevación local de privilegios y puede ser utilizada por un atacante con acceso previo al equipo para obtener permisos elevados.

Recomendaciones de detección

1. **Validar la versión del motor de Microsoft Defender:**
   - Revisar que los endpoints cuenten con una versión corregida del Microsoft Malware Protection Engine.
   - Priorizar la revisión de equipos críticos, servidores, estaciones administrativas, equipos de usuarios privilegiados y dispositivos con acceso a información sensible.
2. **Monitorear eventos de elevación de privilegios:**
   - Revisar eventos anómalos donde procesos de usuario escalen a privilegios de administrador local o SYSTEM.
   - Correlacionar inicios de sesión sospechosos, creación de procesos elevados y cambios no autorizados en servicios del sistema.
3. **Revisar alertas de Microsoft Defender y EDR/XDR:**
   - Analizar eventos relacionados con manipulación de Microsoft Defender, cambios en configuración de protección, desactivación de módulos, exclusiones no autorizadas o errores repetitivos del servicio antimalware.

- Verificar alertas asociadas a tampering, ejecución sospechosa desde rutas temporales o comportamiento anómalo del motor de protección.

4. **Monitorear abuso de enlaces simbólicos, junctions o reparse points:**
   - Debido a que la vulnerabilidad está relacionada con una resolución incorrecta de enlaces antes del acceso a archivos, se recomienda revisar creación o modificación inusual de enlaces simbólicos, junctions o rutas redireccionadas en estaciones Windows.
5. **Revisar actividad posterior a la explotación:**
   - Creación de usuarios locales no autorizados.
   - Inclusión de cuentas en grupos privilegiados.
   - Modificación de servicios, tareas programadas o claves de registro para persistencia.
   - Instalación de herramientas de administración remota no autorizadas.
   - Desactivación de controles de seguridad o creación de exclusiones en Defender.
6. **Fortalecer el monitoreo en activos críticos del sector salud:**
   - Priorizar servidores de historia clínica electrónica, sistemas de información hospitalaria, facturación, laboratorio, imágenes diagnósticas, plataformas de atención al usuario y equipos administrativos con acceso a datos sensibles.

Recomendaciones de mitigación

1. **Aplicar actualizaciones oficiales de Microsoft de forma prioritaria:**
   - Actualizar Microsoft Defender y el Microsoft Malware Protection Engine a versiones corregidas.
   - Validar que las actualizaciones automáticas estén habilitadas y funcionando correctamente.

- En equipos sin conexión permanente a Internet, aplicar mecanismos internos de actualización mediante WSUS, Microsoft Configuration Manager, Intune u otra solución corporativa.

2. **Verificar manualmente el estado de protección:**
   - Confirmar que Microsoft Defender esté activo, actualizado y sin errores de servicio.
   - Revisar que la protección en tiempo real, protección entregada por la nube y protección contra alteraciones estén habilitadas.
3. **Habilitar protección contra alteraciones:**
   - Activar Tamper Protection para reducir la posibilidad de que un atacante deshabilite Microsoft Defender o modifique sus configuraciones críticas después de elevar privilegios.
4. **Restringir privilegios locales:**
   - Aplicar el principio de mínimo privilegio.
   - Evitar que usuarios finales operen con cuentas de administrador local.
   - Revisar periódicamente miembros de grupos como Administradores locales, Usuarios de escritorio remoto y Operadores de copia de seguridad.
5. **Reducir superficie de ataque en endpoints:**
   - Bloquear ejecución desde rutas temporales o no confiables cuando sea posible.
   - Aplicar reglas de reducción de superficie de ataque, control de aplicaciones, listas permitidas y políticas de ejecución seguras.
   - Limitar herramientas administrativas que puedan ser abusadas por atacantes.
6. **Gestionar vulnerabilidades por criticidad:**
   - Incluir CVE-2026-41091 dentro del proceso de gestión de vulnerabilidades con prioridad alta.
   - Verificar cobertura en inventario de activos, estado de parcheo, responsable técnico y fecha de remediación.
7. **Aislar equipos sospechosos:**

- Si se detectan indicios de explotación, aislar el endpoint de la red mediante EDR o control de red.
- Preservar evidencia antes de reinstalar, limpiar o reiniciar sistemas críticos.

8. **Revisar credenciales expuestas:**
   - En caso de compromiso confirmado, restablecer credenciales de usuarios que hayan iniciado sesión en el equipo afectado.
   - Revisar sesiones activas, tokens, credenciales almacenadas y accesos a recursos compartidos.
9. **Actualizar controles de detección:**
   - Ajustar reglas SIEM/EDR para detectar cambios anómalos en Defender, escalamiento de privilegios, creación de tareas programadas, modificación de servicios y creación de cuentas privilegiadas.
10. **Comunicar y hacer seguimiento:**

- Informar a las áreas de tecnología, seguridad, soporte y continuidad del negocio sobre la criticidad de la vulnerabilidad.
- Mantener evidencia del proceso de actualización, verificación y cierre de hallazgos para auditoría interna y cumplimiento.

Conclusiones

CVE-2026-41091 representa una vulnerabilidad crítica de elevación de privilegios local en Microsoft Defender, con riesgo alto para endpoints corporativos y sistemas que manejan información sensible, incluyendo el sector salud. La explotación de esta falla permite a un atacante local ejecutar código con privilegios elevados, evadir controles de seguridad y comprometer la integridad del sistema, así como la confidencialidad de datos críticos.

Dada la naturaleza zero-day de esta vulnerabilidad y su inclusión en el catálogo de CISA KEV como explotada, es esencial que las organizaciones apliquen de inmediato las actualizaciones de Microsoft Defender, refuercen los controles de privilegios locales, implementen monitoreo activo de eventos de seguridad y aseguren la integridad de sus endpoints críticos.

La mitigación temprana y la concienciación sobre esta vulnerabilidad reducirán significativamente el riesgo de explotación y contribuirán a la protección de activos críticos y datos sensibles del ecosistema digital, cumpliendo con estándares de seguridad y normativa vigente en el sector salud.

Fuentes:

- **NVD - National Vulnerability Database:** CVE-2026-41091 detalle oficial de la vulnerabilidad y puntaje CVSS. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2026-41091
- **CISA KEV Catalog:** Inclusión de CVE-2026-41091 como vulnerabilidad explotada conocida y guía de mitigación. Disponible en: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Microsoft Security Response Center (MSRC):** Boletín de seguridad y actualizaciones para Microsoft Defender. Disponible en: https://msrc.microsoft.com/update-guide
- **SecurityWeek:** Reporte de explotación zero-day en Microsoft Defender. Disponible en: https://www.securityweek.com/microsoft-patches-exploited-undefend-and-redsun-defender-zero-days
- **MITRE ATT&CK Framework:** Referencia de técnicas asociadas a la explotación de privilegios y evasión de defensas. Disponible en: https://attack.mitre.org/

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.