

Alerta ID:	133
Fecha del reporte:	13/08/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Grupo Lazarus explota vulnerabilidad de día cero en Windows para elevar privilegios y desplegar el rootkit FudModule
Herramienta de detección	N/A
Activos involucrados:	Estaciones de trabajo y servidores Windows que no hayan instalado las actualizaciones de seguridad de agosto de 2026
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del sector salud sobre la explotación activa de la vulnerabilidad identificada como **CVE-2026-68820**, presente en el controlador **Ancillary Function Driver for WinSock (AFD.sys)** de Microsoft Windows. La vulnerabilidad habría sido utilizada como día cero por el grupo de amenazas **Lazarus**, vinculado a la República Popular Democrática de Corea, durante ataques dirigidos contra organizaciones del sector defensa.

La explotación permite que un atacante que haya obtenido acceso inicial y capacidad de ejecución de código en un sistema vulnerable eleve sus privilegios hasta el nivel **NT AUTHORITY\SYSTEM**. Este nivel de acceso podría facilitar la desactivación o evasión de controles de seguridad, la manipulación de procesos del sistema, el acceso a información sensible y el despliegue de componentes maliciosos con capacidades de rootkit.

Esta alerta busca orientar la identificación de activos potencialmente afectados, la instalación prioritaria de las actualizaciones de seguridad publicadas por Microsoft, la búsqueda de evidencias relacionadas con la explotación de la vulnerabilidad y el fortalecimiento de los controles de prevención, detección y respuesta en los entornos Windows de las entidades del sector salud.



Descripción:

Microsoft corrigió una vulnerabilidad de elevación de privilegios en el controlador de modo kernel **Windows Ancillary Function Driver for WinSock (AFD.sys)**, componente encargado de proporcionar soporte para operaciones de red basadas en sockets dentro del sistema operativo.

La vulnerabilidad, registrada como **CVE-2026-68820**, corresponde a una condición de **uso después de liberar memoria —use-after-free—**. Esta debilidad puede provocar que el controlador continúe utilizando una región de memoria después de que haya sido liberada, lo que permite alterar el flujo de ejecución dentro del contexto del kernel.

Para aprovechar la vulnerabilidad, el atacante debe contar previamente con acceso al equipo y con capacidad para ejecutar código local. Por lo tanto, la falla no constituye por sí sola un mecanismo de acceso inicial remoto. Su función dentro de una cadena de ataque consiste en elevar los privilegios disponibles desde una cuenta o proceso comprometido hasta **SYSTEM**, el nivel de privilegio más alto del sistema operativo Windows.

De acuerdo con la información divulgada, el grupo Lazarus habría incorporado la vulnerabilidad en operaciones dirigidas contra organizaciones del sector defensa. La explotación se habría utilizado para obtener ejecución privilegiada en el kernel y desplegar **FudModule**, un rootkit avanzado diseñado para interferir con los mecanismos de monitoreo y reducir la visibilidad de las soluciones de seguridad instaladas en el sistema.

Una vez ejecutado con privilegios elevados, FudModule puede manipular componentes internos del sistema operativo, ocultar actividad maliciosa y dificultar la detección de las etapas posteriores del ataque. Esta capacidad incrementa el riesgo de persistencia, extracción de información, robo de credenciales y desplazamiento lateral hacia otros activos de la organización.

Microsoft publicó la corrección correspondiente dentro de las actualizaciones de seguridad de agosto de 2026. Debido a que existe evidencia de explotación en ataques reales, la



vulnerabilidad debe tratarse como una prioridad de remediación, independientemente de que su puntuación CVSS no alcance la categoría crítica.

Vulnerabilidad con evidencia de explotación



La vulnerabilidad **CVE-2026-68820** afecta al controlador **Windows Ancillary Function Driver for WinSock (AFD.sys)**, componente del kernel responsable de administrar operaciones de red y de actuar como interfaz entre las aplicaciones que utilizan WinSock y la pila de red de Windows.

La falla se origina en una condición de **uso después de liberar memoria —CWE-416: Use After Free—**. Bajo determinadas condiciones, un proceso local puede provocar que el controlador acceda a un objeto de memoria que ya fue liberado. La manipulación posterior de esa región podría permitir que datos controlados por el atacante sean interpretados dentro del contexto del kernel.

La vulnerabilidad tiene una puntuación **CVSS de 7,0 sobre 10** y fue clasificada por Microsoft con severidad **importante**. Sin embargo, su explotación activa, la capacidad de alcanzar privilegios **SYSTEM** y su integración en operaciones atribuidas a un actor avanzado justifican que las entidades la gestionen con un nivel de riesgo **alto**.

Descripción:

La explotación de CVE-2026-68820 requiere que el atacante haya obtenido previamente capacidad de ejecución de código en el sistema objetivo. Este acceso inicial podría proceder de técnicas como spear phishing, explotación de otra vulnerabilidad, ejecución de archivos maliciosos, abuso de credenciales o compromiso de herramientas de acceso remoto.

Después de obtener ejecución local, el atacante puede interactuar con el controlador AFD.sys y provocar la condición de corrupción de memoria. La explotación exitosa permite ejecutar



código en modo kernel o elevar los privilegios del proceso comprometido hasta **NT AUTHORITY\SYSTEM**.

La vulnerabilidad no debe interpretarse como una falla de ejecución remota de código accesible directamente desde Internet. Corresponde a un mecanismo de **elevación local de privilegios**, utilizado después del compromiso inicial para superar las restricciones de una cuenta con privilegios limitados y obtener control ampliado sobre el sistema operativo.

De acuerdo con la investigación divulgada, Lazarus utilizó esta capacidad para desplegar una variante del rootkit **FudModule**. A diferencia de técnicas de tipo **Bring Your Own Vulnerable Driver —BYOVD—**, en las que el atacante introduce un controlador legítimo pero vulnerable, esta operación aprovechó una vulnerabilidad presente en un controlador nativo de Windows. Esto reduce la necesidad de instalar controladores adicionales y puede dificultar la identificación temprana de la cadena de ataque.

La ejecución en modo kernel permite al componente malicioso interactuar con estructuras internas del sistema operativo y afectar la visibilidad de los mecanismos de protección. Dependiendo de la variante desplegada y del entorno comprometido, esta capacidad puede utilizarse para interferir con soluciones EDR/XDR, ocultar procesos o archivos, manipular telemetría y proteger otros componentes de la operación maliciosa.

Impacto:

La explotación exitosa de CVE-2026-68820 podría comprometer la confidencialidad, integridad y disponibilidad de los sistemas Windows afectados. Un atacante podría:

- Elevar privilegios desde una cuenta o proceso local hasta **NT AUTHORITY\SYSTEM**.
- Ejecutar código con privilegios de kernel.
- Acceder a archivos, credenciales, tokens de acceso y configuraciones protegidas.
- Manipular procesos, servicios y componentes internos del sistema operativo.
- Deshabilitar, evadir o interferir con soluciones antivirus, EDR/XDR y otros mecanismos de monitoreo.



- Instalar rootkits, puertas traseras y mecanismos de persistencia con privilegios elevados.
- Ocultar procesos, archivos, conexiones o actividad maliciosa.
- Modificar configuraciones de seguridad, auditoría y registro de eventos.
- Extraer información sensible almacenada o procesada en el equipo comprometido.
- Utilizar credenciales y sesiones activas para desplazarse lateralmente hacia otros sistemas.
- Mantener acceso persistente al entorno institucional y facilitar operaciones posteriores de espionaje o sabotaje.

El impacto puede ser mayor en controladores de dominio, servidores de aplicaciones, estaciones administrativas, equipos utilizados por personal con privilegios elevados y dispositivos desde los cuales se accede a sistemas clínicos, financieros o administrativos.

Estado de explotación:

Existe evidencia pública de explotación activa de **CVE-2026-68820** antes de que la actualización de seguridad estuviera disponible, condición por la cual se considera una vulnerabilidad de día cero.

La actividad observada ha sido atribuida al grupo **Lazarus**, actor de amenazas persistentes avanzadas asociado públicamente con intereses del Gobierno de Corea del Norte. Las operaciones reportadas estuvieron dirigidas principalmente contra organizaciones del sector defensa y utilizaron la vulnerabilidad como parte de una cadena de ataque orientada a obtener privilegios elevados y desplegar el rootkit FudModule.

La atribución de una campaña a Lazarus no implica que la vulnerabilidad permanezca limitada a los objetivos inicialmente observados. Después de la publicación del identificador CVE y de la corrección de seguridad, otros actores pueden analizar las diferencias entre las versiones vulnerables y corregidas, desarrollar nuevos mecanismos de explotación y reutilizarlos contra organizaciones que no hayan instalado las actualizaciones.



A la fecha de elaboración de esta alerta, no se ha confirmado públicamente que las entidades del sector salud hayan sido objetivo específico de esta campaña. No obstante, la presencia generalizada de Windows, el valor de la información clínica y personal, y la dependencia de servicios tecnológicos críticos hacen necesario tratar la vulnerabilidad como una amenaza relevante para el sector.

Las entidades deben priorizar la instalación de las actualizaciones de seguridad, verificar posibles indicadores de compromiso y revisar cualquier alerta relacionada con elevación de privilegios, manipulación del kernel o interferencia con los controles de seguridad.

Productos y versiones afectadas

CVE-2026-68820 afecta las versiones de Microsoft Windows que incorporan una versión vulnerable del controlador AFD.sys y que no cuentan con las actualizaciones de seguridad publicadas por Microsoft en agosto de 2026.

Deben considerarse potencialmente afectados los siguientes productos cuando no tengan instalada la actualización acumulativa correspondiente:

- Windows 10 bajo programas de soporte o actualizaciones de seguridad extendidas.
- Windows 11 en sus diferentes versiones y arquitecturas compatibles.
- Windows Server 2012 y Windows Server 2012 R2 bajo programas de actualizaciones de seguridad extendidas.
- Windows Server 2016.
- Windows Server 2019.
- Windows Server 2022.
- Windows Server 2025.
- Instalaciones Server Core de las versiones afectadas de Windows Server.

La relación exacta de versiones, arquitecturas, compilaciones y paquetes de actualización debe verificarse en la matriz de productos afectados publicada por Microsoft para **CVE-2026-68820**. Las entidades deben validar la remediación mediante el número de compilación y la



actualización acumulativa instalada, no únicamente mediante el nombre comercial del sistema operativo.

El componente vulnerable forma parte del sistema operativo y no requiere que el equipo tenga instalado software de terceros. Por esta razón, la evaluación de exposición debe abarcar estaciones de trabajo, equipos portátiles, servidores físicos, máquinas virtuales y otros activos Windows administrados por la entidad.

La presencia del controlador AFD.sys no constituye por sí sola un indicador de compromiso, debido a que corresponde a un archivo legítimo de Windows. El riesgo se presenta cuando el sistema utiliza una versión vulnerable del controlador y un atacante ya dispone de capacidad para ejecutar código local.

Activos con mayor exposición

Aunque la vulnerabilidad requiere acceso local previo, su explotación puede transformar un compromiso con privilegios limitados en una intrusión con control completo sobre el sistema. La prioridad debe establecerse considerando la función del activo, los privilegios disponibles, la sensibilidad de la información procesada y la exposición a mecanismos de acceso inicial.

Se deben priorizar los siguientes activos:

- Controladores de dominio y servidores que prestan servicios de identidad, autenticación o directorio.
- Servidores de aplicaciones clínicas, administrativas, financieras o asistenciales.
- Equipos desde los cuales se administran infraestructuras, redes, bases de datos, plataformas de virtualización o servicios de seguridad.
- Estaciones utilizadas por administradores de dominio, personal de soporte o usuarios con privilegios elevados.
- Equipos que almacenan o procesan historias clínicas, datos personales, información financiera o documentación institucional reservada.
- Dispositivos empleados para acceder a sistemas de información hospitalaria, historias clínicas electrónicas, PACS, RIS, LIS y plataformas de telemedicina.



- Servidores y estaciones con acceso a segmentos que alojan dispositivos médicos o tecnologías operacionales.
- Equipos que presentan alertas previas de ejecución de código, malware, robo de credenciales o acceso remoto no autorizado.
- Sistemas sin cobertura de EDR/XDR o con agentes de seguridad deshabilitados, desactualizados o sin comunicación con la consola central.
- Dispositivos que no reciben actualizaciones mediante mecanismos centralizados como WSUS, Microsoft Intune, Configuration Manager o plataformas equivalentes.
- Sistemas con versiones de Windows fuera de soporte o dependientes de aplicaciones que impiden instalar oportunamente las actualizaciones.
- Equipos accesibles mediante RDP, VPN, herramientas de soporte remoto u otros servicios de administración.
- Activos que permiten la ejecución de archivos descargados, adjuntos de correo o herramientas no autorizadas.

La prioridad más alta corresponde a los activos en los que coincidan una versión vulnerable, evidencias de acceso inicial y señales de actividad posterior orientada a obtener privilegios elevados.

Consideraciones para el sector salud

Las entidades del sector salud operan infraestructuras Windows utilizadas para soportar procesos clínicos, administrativos, financieros, farmacéuticos, de laboratorio, diagnóstico por imágenes y atención remota. El compromiso de estos sistemas puede afectar tanto la protección de la información como la continuidad de los servicios asistenciales.

La explotación de CVE-2026-68820 podría permitir que un atacante transforme el acceso obtenido mediante phishing, malware o credenciales comprometidas en control privilegiado del equipo afectado. Desde esta posición, el actor podría acceder a información clínica, extraer credenciales, alterar configuraciones, desactivar controles de seguridad y utilizar el dispositivo como punto de entrada hacia otros segmentos de la red.



El riesgo es especialmente relevante en estaciones utilizadas para administrar plataformas críticas o acceder a múltiples sistemas institucionales. Los tokens, credenciales, certificados y sesiones disponibles en estos equipos pueden facilitar el desplazamiento lateral y ampliar el alcance del incidente.

Los sistemas médicos que dependan de versiones específicas de Windows o que no puedan actualizarse inmediatamente por restricciones de compatibilidad requieren un tratamiento prioritario. La imposibilidad de instalar la corrección debe documentarse formalmente y acompañarse de controles compensatorios, segmentación de red, restricción de ejecución, monitoreo reforzado y aislamiento de los servicios no indispensables.

La explotación en modo kernel también puede reducir la eficacia de las herramientas de seguridad instaladas en el dispositivo. Por esta razón, la ausencia de alertas del antivirus o del EDR no debe utilizarse como único criterio para descartar un compromiso. La revisión debe integrar telemetría del endpoint, registros centralizados, eventos de identidad y datos de red.

Un incidente que afecte servidores clínicos, sistemas de imágenes diagnósticas o plataformas de atención podría provocar indisponibilidad, pérdida de trazabilidad, exposición de datos sensibles y retrasos en la prestación de servicios. Las actividades de actualización deben coordinarse con los responsables tecnológicos, clínicos y de continuidad para reducir el riesgo operativo sin aplazar injustificadamente la remediación.

Indicadores de compromiso (IoC) y actividades de detección

La información pública consultada no proporciona un conjunto completo y verificable de indicadores estáticos —direcciones IP, dominios, nombres de archivo o valores hash— que permita identificar por sí solo todas las intrusiones relacionadas con CVE-2026-68820.

La ausencia de indicadores estáticos no impide realizar actividades de detección. Debido a que el exploit puede cambiar entre campañas y el rootkit opera con privilegios elevados, las entidades deben priorizar indicadores de comportamiento, correlación de eventos y búsqueda de anomalías en los sistemas potencialmente afectados.



La presencia de afd.sys no debe considerarse maliciosa. Este es un controlador legítimo de Windows, normalmente ubicado en:

C:\Windows\System32\drivers\afd.sys

La investigación debe concentrarse en interacciones anómalas con el controlador, explotación de memoria, elevación inesperada de privilegios y acciones posteriores ejecutadas como SYSTEM.

Actividades de detección recomendadas:

Se recomienda prestar especial atención a:

- Procesos iniciados por usuarios sin privilegios que posteriormente ejecuten acciones bajo el contexto NT AUTHORITY\SYSTEM.
- Cambios inesperados en el nivel de integridad o en el token de seguridad de un proceso.
- Procesos no habituales que generen una cantidad anómala de operaciones sobre sockets o dispositivos asociados con AFD.
- Alertas del EDR/XDR relacionadas con explotación de kernel, corrupción de memoria, uso después de liberar memoria o elevación local de privilegios.
- Carga de código no firmado o no reconocido en procesos con privilegios elevados.
- Creación de servicios, controladores o tareas programadas después de una alerta de ejecución sospechosa.
- Acceso inusual a objetos del kernel desde procesos de usuario no autorizados.
- Terminación, suspensión o manipulación de procesos pertenecientes a soluciones antivirus, EDR/XDR, agentes de monitoreo o herramientas de administración.
- Desactivación de Microsoft Defender Antivirus, protección contra alteraciones, registro de eventos, AMSI o controles de auditoría.
- Modificación inesperada de exclusiones de Microsoft Defender o de políticas aplicadas a las soluciones de seguridad.
- Pérdida simultánea de telemetría de varios componentes de protección en un mismo equipo.



- Reinicios o fallos del sistema próximos a eventos de ejecución de archivos desconocidos, corrupción de memoria o actividad sospechosa de red.
- Creación o modificación de archivos dentro de C:\Windows\System32\drivers\ y otros directorios protegidos.
- Carga de controladores desde rutas diferentes a los directorios legítimos de Windows.
- Ejecución de herramientas de volcado de credenciales, reconocimiento de dominio, manipulación de tokens o inyección de procesos después de la elevación de privilegios.
- Conexiones salientes iniciadas por procesos que normalmente no requieren acceso a Internet.
- Accesos laterales mediante SMB, RDP, WinRM, WMI, PsExec o tareas programadas desde el equipo potencialmente comprometido.

Existe evidencia pública de explotación activa de **CVE-2026-68820** antes de que la actualización de seguridad estuviera disponible, condición por la cual se considera una vulnerabilidad.

Registros y eventos de interés:

Las entidades deben correlacionar, cuando se encuentren habilitados, los siguientes registros:

- **Evento 4688:** creación de procesos, especialmente cuando el proceso resultante se ejecute con privilegios elevados o bajo la cuenta SYSTEM.
- **Evento 4672:** asignación de privilegios especiales a un nuevo inicio de sesión.
- **Eventos 4624 y 4625:** inicios de sesión exitosos y fallidos, incluidos accesos remotos o desde orígenes no habituales.
- **Evento 4697:** instalación de un servicio en el sistema.
- **Evento 7045:** creación de un nuevo servicio registrada por Service Control Manager.
- **Evento 4698:** creación de una tarea programada.
- **Eventos 1102 y 104:** eliminación del registro de auditoría o de otros registros de eventos.
- **Evento 4719:** modificación de la política de auditoría.



- **Eventos 5001 y 5004:** cambios en el estado o en la configuración de Microsoft Defender Antivirus.
- **Evento 5007:** modificación de la configuración de Microsoft Defender.
- **Eventos de Sysmon 1, 3, 6, 7, 10, 11 y 13:** creación de procesos, conexiones de red, carga de controladores, carga de imágenes, acceso entre procesos, creación de archivos y modificaciones del Registro.

Los identificadores de eventos deben analizarse dentro de su contexto. Su presencia aislada no confirma una explotación, pero la combinación de ejecución sospechosa, elevación a SYSTEM, carga de componentes y pérdida de telemetría incrementa la probabilidad de compromiso.

Búsqueda de actividad asociada con FudModule:

Las capacidades de FudModule pueden variar entre versiones. Las actividades de búsqueda deben enfocarse en comportamientos compatibles con un rootkit en modo kernel, entre ellos:

- Procesos visibles en telemetría de red o registros externos que no aparezcan en las herramientas locales de enumeración.
- Archivos existentes en disco que no sean presentados por las interfaces habituales del sistema.
- Conexiones de red activas sin un proceso local claramente asociado.
- Diferencias entre los resultados obtenidos desde el sistema operativo y los registros recopilados por sensores externos.
- Controladores cargados sin información válida de firma o procedencia.
- Manipulación de callbacks, filtros o estructuras utilizadas por los mecanismos de seguridad.
- Procesos de seguridad terminados, suspendidos o desconectados sin una acción administrativa autorizada.
- Ausencia repentina de eventos en un equipo que previamente generaba telemetría de manera regular.



- Artefactos en memoria que no correspondan con módulos registrados formalmente por el sistema operativo.

Para activos de alta criticidad, se recomienda realizar adquisición y análisis de memoria. Los rootkits pueden ocultar artefactos frente a las herramientas ejecutadas dentro del sistema comprometido, por lo que el análisis basado exclusivamente en archivos puede resultar insuficiente.

Criterios de escalamiento:

Se debe iniciar el procedimiento institucional de respuesta a incidentes cuando se identifique una o varias de las siguientes condiciones:

- Un sistema vulnerable presenta una alerta de explotación de kernel o elevación de privilegios.
- Un proceso no autorizado obtiene privilegios SYSTEM.
- La solución EDR/XDR deja de reportar después de una ejecución sospechosa.
- Se detecta carga de controladores desconocidos o manipulación de mecanismos de protección.
- Existen diferencias entre la telemetría local y los registros externos.
- Se observan movimientos laterales o accesos a sistemas críticos desde el equipo investigado.
- Se identifican herramientas, comandos o artefactos relacionados con robo de credenciales, persistencia o evasión de defensas.

Los hallazgos deben compararse con las ventanas de mantenimiento, actividades de soporte y cambios autorizados. Cuando la actividad no pueda justificarse, se deben preservar las evidencias, aislar el activo e iniciar el análisis forense correspondiente.



Medidas de Prevención



Para reducir el riesgo asociado con CVE-2026-68820, las entidades deben instalar las actualizaciones de seguridad publicadas por Microsoft en agosto de 2026 y fortalecer los controles que dificultan la obtención de acceso inicial y la ejecución de código no autorizado. Se recomienda implementar las siguientes medidas:

- Instalar de manera prioritaria la actualización acumulativa de agosto de 2026 correspondiente a cada versión y arquitectura de Windows.
- Verificar la instalación mediante el número de compilación, el paquete KB aplicado y la información reportada por las herramientas de administración de vulnerabilidades.
- Reiniciar los sistemas cuando la actualización lo requiera y comprobar posteriormente que el equipo no mantenga actualizaciones pendientes.
- Incluir estaciones de trabajo, servidores, máquinas virtuales, plantillas de imágenes y equipos que permanezcan desconectados durante los ciclos normales de actualización.
- Actualizar las imágenes maestras utilizadas para desplegar estaciones de trabajo y servidores.
- Mantener habilitada la protección contra alteraciones de Microsoft Defender o la funcionalidad equivalente de la solución EDR/XDR.
- Utilizar Windows Defender Application Control, AppLocker u otros mecanismos de control de aplicaciones para limitar la ejecución de código no autorizado.
- Restringir la ejecución de scripts, binarios y bibliotecas desde directorios temporales, perfiles de usuario y ubicaciones susceptibles de escritura.
- Implementar reglas de reducción de superficie de ataque —ASR— para bloquear comportamientos asociados con archivos maliciosos, robo de credenciales y abuso de aplicaciones legítimas.
- Proteger las credenciales administrativas mediante cuentas separadas, estaciones de acceso privilegiado y mecanismos de autenticación multifactor.
- Limitar el acceso mediante RDP, WinRM, WMI, SMB y herramientas de soporte remoto a redes y cuentas expresamente autorizadas.
- Deshabilitar servicios, protocolos y herramientas de administración que no sean necesarios.



- Mantener actualizados Microsoft Defender Antivirus, los motores de detección, las firmas y los agentes EDR/XDR.
- Centralizar la telemetría de endpoints, identidad, red y autenticación en una plataforma SIEM.
- Configurar alertas ante desactivación de controles de seguridad, elevación de privilegios, carga de controladores y pérdida de comunicación con los agentes.
- Aplicar segmentación de red entre estaciones de usuario, servidores, dispositivos médicos, sistemas clínicos y plataformas administrativas.
- Restringir el tráfico lateral mediante firewall de host y controles de acceso entre segmentos.
- Fortalecer los controles de correo electrónico, navegación y descarga de archivos para reducir las posibilidades de acceso inicial.
- Capacitar al personal sobre campañas de spear phishing, falsas ofertas laborales, solicitudes de soporte y otros mecanismos de ingeniería social utilizados por actores avanzados.

La explotación requiere que el atacante haya conseguido ejecutar código en el equipo. Por esta razón, las medidas de prevención deben cubrir tanto la vulnerabilidad como las etapas anteriores de la cadena de ataque.

Medidas de detección y mitigación

Las entidades deben realizar una revisión centralizada de sus activos Windows para identificar sistemas vulnerables, confirmar la instalación de la actualización y detectar señales de compromiso anteriores a la remediación.

Como parte de esta revisión, se recomienda:

- Elaborar o actualizar el inventario de estaciones y servidores Windows.
- Consultar la matriz de productos afectados publicada por Microsoft para CVE-2026-68820.
- Identificar sistemas que no tengan instalada la actualización acumulativa de agosto de 2026 o una posterior que la reemplace.



- Priorizar activos críticos, servidores, estaciones administrativas y equipos con acceso a información sensible.
- Verificar la versión y firma digital de C:\Windows\System32\drivers\afd.sys.
- Comparar el hash y la versión del controlador con los valores correspondientes a una compilación legítima y actualizada del mismo sistema operativo.
- Revisar alertas históricas de EDR/XDR generadas antes de instalar la actualización.
- Buscar eventos de elevación de privilegios, corrupción de memoria, explotación de kernel y ejecución bajo el contexto SYSTEM.
- Analizar cambios en servicios, tareas programadas, controladores, exclusiones de seguridad y políticas de auditoría.
- Identificar equipos cuya solución de seguridad haya dejado de reportar de forma inesperada.
- Correlacionar eventos del endpoint con registros de autenticación, proxy, DNS, firewall, VPN y directorio activo.
- Revisar conexiones laterales realizadas desde sistemas potencialmente comprometidos.
- Realizar análisis de memoria en activos que presenten indicios compatibles con rootkits o manipulación del kernel.
- Verificar la integridad de los agentes de seguridad y reinstalarlos cuando no pueda garantizarse su funcionamiento.
- Conservar la telemetría y las evidencias antes de ejecutar acciones que puedan modificar los artefactos del sistema.

Cuando un equipo no pueda actualizarse inmediatamente, deben aplicarse controles compensatorios. Estos controles reducen la exposición, pero no sustituyen la instalación de la corrección.

Se recomienda:

- Aislar el equipo en un segmento restringido.
- Impedir el acceso directo a Internet cuando no sea indispensable.
- Limitar las conexiones entrantes y salientes a los servicios estrictamente necesarios.
- Bloquear la ejecución de aplicaciones no autorizadas.
- Retirar temporalmente privilegios administrativos locales.



- Restringir el acceso mediante RDP, SMB, WinRM, WMI y herramientas de soporte remoto.
- Incrementar el nivel de registro y monitoreo.
- Supervisar continuamente el estado del EDR/XDR.
- Evitar que el equipo sea utilizado para tareas administrativas o acceso a sistemas críticos.
- Establecer una fecha límite de remediación aprobada por los responsables de seguridad y del servicio.

No se ha identificado una mitigación de configuración que elimine por completo la vulnerabilidad del controlador afectado. La medida correctiva principal es instalar la actualización de seguridad publicada por Microsoft.

Respuesta ante una posible explotación

Cuando se identifiquen indicios de elevación a SYSTEM, manipulación del kernel, despliegue de rootkits o interferencia con las soluciones de seguridad, la entidad debe activar inmediatamente su procedimiento de respuesta a incidentes.

Se recomienda ejecutar las siguientes acciones:

- Aislar el equipo potencialmente comprometido mediante la consola EDR/XDR o controles de red.
- Evitar el apagado o reinicio inmediato cuando se requiera preservar artefactos residentes en memoria.
- Adquirir una imagen de memoria antes de ejecutar acciones de erradicación, siempre que las capacidades institucionales lo permitan.
- Preservar los registros de Windows, EDR/XDR, SIEM, firewall, DNS, proxy, VPN y autenticación.
- Registrar la fecha, hora, usuario, dirección IP y proceso relacionados con la actividad sospechosa.
- Identificar el mecanismo utilizado para obtener acceso inicial al sistema.



- Determinar qué proceso explotó la vulnerabilidad y qué acciones fueron ejecutadas después de obtener privilegios SYSTEM.
- Revisar la carga de controladores, servicios, tareas programadas y mecanismos de persistencia.
- Examinar los procesos y conexiones de red mediante fuentes externas al sistema comprometido.
- Identificar cuentas, contraseñas, tokens, certificados y sesiones que pudieron quedar expuestos.
- Restablecer las credenciales comprometidas desde un dispositivo confiable.
- Revocar sesiones, tokens y certificados cuando exista riesgo de uso no autorizado.
- Analizar los sistemas a los que se accedió desde el equipo comprometido.
- Buscar actividad similar en otros dispositivos con la misma configuración o pertenecientes al mismo segmento.
- Aplicar las actualizaciones de seguridad antes de reincorporar el equipo a la red.
- Restaurar o reconstruir el sistema desde una imagen confiable cuando no sea posible garantizar la eliminación del rootkit.
- Evitar depender únicamente de una limpieza realizada desde el propio sistema comprometido.
- Validar el funcionamiento de los controles de seguridad después de la recuperación.
- Mantener el activo bajo monitoreo reforzado después de su reincorporación.
- Documentar los hallazgos, decisiones, acciones ejecutadas y evidencias recolectadas.
- Reportar el incidente al equipo institucional responsable de seguridad digital y seguir los canales de notificación aplicables.

Debido a que FudModule opera en modo kernel y puede interferir con los mecanismos de visibilidad, la ausencia de artefactos en una revisión convencional no garantiza la integridad del equipo. Cuando existan evidencias razonables de compromiso, la reconstrucción desde una fuente confiable ofrece mayores garantías que la remoción manual.

El restablecimiento del sistema debe realizarse únicamente después de confirmar que la vulnerabilidad fue corregida, las credenciales potencialmente expuestas fueron renovadas, los mecanismos de persistencia fueron eliminados y no existe evidencia de desplazamiento lateral.



Fuentes:

- <https://thehackernews.com/2026/08/lazarus-exploits-windows-zero-day-to.html>
- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820>
- <https://msrc.microsoft.com/update-guide/>
- <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- <https://www.cve.org/CVERecord?id=CVE-2026-68820>

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 **contacto@csirtsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

