vRx Informe de Vulnerabilidades

Fecha de Generación: 20 de julio de 2026
Identificador del Equipo: 1752749
Nombre del Equipo: DEMO
Sistema Operativo: Windows Server 2019
Dirección IP: 75.123.369.25
Nivel de Riesgo: Riesgo Alto
Puntuación de Riesgo: 10 / 10

DEMO

Propósito del informe: Apoyar la gestión de riesgos de ciberseguridad conforme a buenas prácticas promovidas por la Ley 21.663

Este informe contiene un análisis del estado de seguridad del endpoint ubicado en demo, con énfasis en las vulnerabilidades identificadas en el sistema Windows Server 2019. Está dirigido a la gerencia para facilitar la toma de decisiones informadas sobre la gestión de riesgos y la seguridad informática. Se recomienda revisar las métricas y los hallazgos clave para comprender el panorama de seguridad actual.

Generado por: Inteligencia Artificial Tecnoinver | soporte@tecnoinver.cl
Confidencial: Este informe contiene información sensible de seguridad y análisis de vulnerabilidades del equipo DEMO.

Resumen Ejecutivo del Equipo

Análisis del Estado de Seguridad del Equipo

El estado de seguridad del endpoint en demo se califica como de alto riesgo, con un puntaje de riesgo de 10/10. Se identificaron un total de 52 CVEs, de las cuales 3 son críticas, 34 son altas, 8 son medias y 7 son bajas. La alta cantidad de vulnerabilidades críticas y altas resalta una necesidad urgente de atención y gestión. El promedio de CVSS es de 7.42, lo que indica una significativa preocupación por la seguridad del sistema.

Hallazgos Clave

- El endpoint presenta 3 vulnerabilidades críticas en .NET Framework con un CVSS de 9.8.
- Existen 34 vulnerabilidades altas que podrían comprometer la seguridad de la información.
- El endpoint tiene un riesgo significativo de exposición a ataques de tipo RCE y denegación de servicio.
- No se han encontrado parches disponibles para abordar las vulnerabilidades identificadas.

DEMO

TOTAL DE CVES	PROMEDIO CVSS	PUNTUACIÓN DE RIESGO
52	7.42	10

VULNERABILIDADES CRÍTICAS	VULNERABILIDADES ALTAS	VULNERABILIDADES MEDIAS	VULNERABILIDADES BAJAS
3	34	8	7

¿Qué significan estas métricas?

CVE: Es un identificador oficial de una vulnerabilidad pública (por ejemplo: CVE-2024-XXXXX), registrada en bases como NIST/NVD. Cada CVE representa una debilidad real detectada en software o sistema operativo.

CVSS: Es el puntaje estándar internacional (de 0 a 10) que indica qué tan grave es una vulnerabilidad. Mientras más alto el puntaje, mayor es el impacto potencial.

Clasificación CVSS: Bajo (0.0 – 3.9) Medio (4.0 – 6.9) Alto (7.0 – 8.9) Crítico (9.0 – 10.0)

Nota: El riesgo final mostrado por vRx considera severidad (CVEs) + factores técnicos del activo (xTags), lo que permite priorizar vulnerabilidades realmente explotables en el entorno.

DEMO

Vulnerabilidades - Análisis Detallado

Las siguientes vulnerabilidades representan los mayores riesgos para este equipo. Cada una incluye una

explicación ejecutiva de su impacto potencial y las acciones recomendadas para su mitigación inmediata.

CVE-2020-0646

CVSS 9.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

Este fallo permite a un atacante remoto ejecutar código no autorizado si envía entradas mal formadas al componente afectado. La explotación no requiere interacción del usuario y podría ocurrir a través de servicios expuestos.

Impacto en el Negocio:

Podría comprometer la confidencialidad, integridad y disponibilidad de los sistemas, permitiendo acceso no autorizado y control de servicios clave. Esto podría interrumpir operaciones críticas, generar interrupciones en la disponibilidad de aplicaciones y afectar la confianza de clientes y socios. A nivel reputacional podría haber impactos si se reportan fallos repetidos o incidentes.

Acción Recomendada:

Aplicar de inmediato el parche correspondiente y validar la corrección en entornos de pruebas antes de desplegar en producción. El equipo de Infraestructura y Seguridad debe coordinar un parcheo controlado en ventanas de mantenimiento, realizar pruebas de regresión y monitorizar logs para detectar intentos de explotación.

DEMO

CVE-2023-36049

CVSS 9.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

Este fallo permite a un atacante con privilegios elevados obtener control adicional sobre el sistema al escalar privilegios dentro de la plataforma. La explotación podría realizarse con capacidades ya presentes en el entorno.

Impacto en el Negocio:

Un aumento de privilegios podría facilitar acceso a información sensible, alterar configuraciones y causar interrupciones operativas. Esto incrementa el riesgo de abuso interno, compromete la integridad de procesos y puede generar costos de remediación y retrabajo. También puede complicar auditorías y cumplimiento por acceso no autorizado.

Acción Recomendada:

Aplicar el parche de Microsoft y verificar la versión afectada en todos los entornos. Revisar y reforzar políticas de privilegios (principio de mínimo privilegio), emitir alerts para actividad anómala y realizar pruebas de escalamiento en un entorno seguro.

DEMO

CVE-2024-0057

CVSS 9.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Este fallo permite saltar controles de seguridad en ciertas operaciones de .NET Framework y Visual Studio, facilitando acciones no autorizadas.

Impacto en el Negocio:
Puede afectar la confiabilidad de la plataforma, permitir cambios no autorizados y exponer información sensible. La explotación podría impactar la continuidad de servicios y generar costs por investigación y mitigación. También puede afectar la confianza de clientes y socios si se percibe debilidad en controles de seguridad.

Acción Recomendada:
Aplicar el parche del fabricante y validar que los controles de seguridad estén activos tras la actualización. Revisar configuraciones de seguridad y realizar pruebas de validación en un entorno de pruebas antes de mover a producción.

DEMO

CVE-2019-1113

CVSS 8.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Existe la posibilidad de ejecutar código de forma remota si se procesa mal la entrada de un archivo, permitiendo tomar control del sistema afectado.

Impacto en el Negocio:
Podría exponer datos o interrumpir servicios, afectando procesos críticos y la continuidad operativa. Se incrementa el riesgo de comprometer la confidencialidad y la integridad de información sensible.

Acción Recomendada:
Aplicar el parche correspondiente y asegurar validaciones de entrada en XML/archivo relevante. Coordinar con Infraestructura para pruebas de compatibilidad y despliegue controlado, seguido de monitoreo de seguridad y eventos inusuales.

CVE-2020-0606

CVSS 8.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo que podría permitir ejecución remota de código cuando se procesan entradas en archivos, si se aprovecha adecuadamente.

Impacto en el Negocio:
Puede resultar en control no autorizado de sistemas y exposición de datos, con impacto en operaciones y reputación. La explotación podría interrumpir servicios o afectar la disponibilidad de aplicaciones críticas.

Acción Recomendada:
Descargar e implementar el parche oficial y realizar pruebas de aceptación. Verificar que entornos de producción estén parcheados y habilitar monitoreo de actividad anómala en componentes afectados.

DEMO

CVE-2020-0605

CVSS 8.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Similar a otros fallos de entrada, podría permitir ejecución de código si se aprovecha la mala validación de entradas de archivos.

Impacto en el Negocio:
Riesgo de intrusión, pérdida de datos y interrupciones en servicios. Puede afectar operaciones diarias, generación de informes y disponibilidad de sistemas clave.

Acción Recomendada:
Aplicar parche del proveedor, validar compatibilidad y realizar pruebas de regresión. Contemplar un plan de parcheo en ciclo de mantenimiento y monitorear indicadores de intrusión.

CVE-2023-36899

CVSS 8.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo que permite elevación de privilegios en la capa ASP.NET, posibilitando que un atacante obtenga permisos superiores.

Impacto en el Negocio:
Un atacante podría modificar configuraciones, acceder a datos con mayores privilegios y afectar la operación de la aplicación. Esto incrementa el riesgo de exposición de información y de interrupciones no planificadas.

Acción Recomendada:
Aplicar la corrección y auditar permisos de cuentas que interactúan con ASP.NET. Realizar pruebas de escalamiento en entorno aislado y reforzar controles de acceso.

DEMO

CVE-2023-36560

CVSS 8.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo de saltar controles de seguridad en ASP.NET, permitiendo acciones no autorizadas con relativa facilidad.

Impacto en el Negocio:
Podría conducir a exposición de datos y alteración de procesos, con impacto en la confianza de clientes y continuidad operativa.

Acción Recomendada:
Implementar parche y revisar configuraciones de seguridad. Validar que funciones críticas no queden expuestas y ejecutar pruebas de seguridad en entornos controlados.

CVE-2025-21176

CVSS 8.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

Fallo que facilita ejecución remota de código en .NET Framework, permitiendo control del sistema afectado.

Impacto en el Negocio:

Puede permitir acceso no autorizado, manipulación de datos y caída de servicios, afectando operaciones y reputación.

Acción Recomendada:

Aplicar parche del proveedor y validar en pruebas previas a producción. Monitorear por intentos de explotación y reforzar controles de red hacia los sistemas afectados.

DEMO

CVE-2024-0056

CVSS 8.7

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

Fallo en SQL Data Provider que podría permitir evadir controles de seguridad al acceder a datos.

Impacto en el Negocio:

Riesgo de exposición de datos, accesos no autorizados y alteración de información sensible, con posibles impactos legales y de confianza de clientes.

Acción Recomendada:

Parchear componentes afectados y revisar las configuraciones de acceso a bases de datos. Realizar pruebas de seguridad y controles de auditoría para detectar accesos inusuales.

CVE-2020-1147

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota si se procesa XML de entrada de forma insegura en varias plataformas.

Impacto en el Negocio:
Impacto en disponibilidad y confidencialidad de datos, con posibilidad de interrupciones y filtraciones si se explotan fallos.

Acción Recomendada:
Aplicar parche y endurecer validación de entradas XML. Realizar pruebas en entornos no productivos y monitorizar tráfico hacia servicios afectados.

DEMO

CVE-2022-26929

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo que facilita ejecución remota de código, permitiendo toma de control si se explota la debilidad.

Impacto en el Negocio:
Puede implicar pérdida de control sobre sistemas, exposición de datos y disrupciones operativas, afectando continuidad y confianza.

Acción Recomendada:
Aplicar parche, validar versiones y realizar pruebas de caída de servicio. Reforzar monitoreo de operaciones y control de accesos en entornos expuestos.

CVE-2022-41089

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código en la plataforma afectada, permitiendo control no autorizado.

Impacto en el Negocio:
Podría impactar la disponibilidad de servicios, exponer datos y generar interrupciones operativas prolongadas. Afecta la reputación ante clientes y socios.

Acción Recomendada:
Desplegar parche oficial y validar en entornos de prueba. Planificar parcheo coordinado y monitorear intentos de explotación en producción.

DEMO

CVE-2023-21808

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo que facilita ejecución remota de código en la pila .NET/Visual Studio.

Impacto en el Negocio:
Riesgo de intrusión, interrupciones y posible filtración de datos en aplicaciones críticas.

Acción Recomendada:
Aplicar parche, probar compatibilidad y actualizar dependencias. Ejecutar controles de seguridad y supervisión de eventos para detectar intentos de explotación.

CVE-2023-29326

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código ante entrada manipulada en la plataforma afectada.

Impacto en el Negocio:
Puede comprometer la continuidad de servicios y la confidencialidad de información sensible, con posibles impactos reputacionales.

Acción Recomendada:
Aplicar parche y validar en pruebas, desplegar en producción siguiendo el plan de mantenimiento, y monitorizar actividad anómala.

DEMO

CVE-2023-24897

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código en la pila .NET/Visual Studio ante entradas específicas.

Impacto en el Negocio:
Posible interrupción de servicios, exposición de información sensible y pérdidas operativas si se explota.

Acción Recomendada:
Parchear, validar compatibilidad y realizar pruebas de regresión. Mantener supervisión de incidentes y controles de acceso a sistemas críticos.

CVE-2023-24895

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código asociada a componentes de desarrollo y runtime.

Impacto en el Negocio:
Puede derivar en interrupciones con impacto en operaciones y posible filtración de datos, afectando la confianza de usuarios.

Acción Recomendada:
Aplicar parche y reforzar controles de seguridad. Validar entornos de desarrollo y producción, con pruebas de regresión y monitoreo de logs.

DEMO

CVE-2023-36796

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código relacionada con Visual Studio.

Impacto en el Negocio:
Podría afectar la continuidad de proyectos y servicios, con posible exposición de datos y fallos en operaciones de desarrollo.

Acción Recomendada:
Parchear y revisar configuraciones de seguridad de Visual Studio en equipos de desarrollo. Ejecutar pruebas de compatibilidad y monitorizar actividad sospechosa.

CVE-2023-36794

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código en Visual Studio.

Impacto en el Negocio:
Puede generar interrupciones operativas y posibles filtraciones de información sensible durante procesos de desarrollo o despliegue.

Acción Recomendada:
Actualizar Visual Studio y componentes relacionados, verificar dependencias y realizar pruebas de seguridad antes de definir despliegues.

DEMO

CVE-2023-36793

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código vinculado a herramientas de desarrollo y runtime.

Impacto en el Negocio:
Impacto potencial en servicios, integridad de datos y plazos de entrega por interrupciones o modificaciones no autorizadas.

Acción Recomendada:
Aplicar parches y validar entornos de desarrollo/producción. Establecer monitoreo continuo de actividades en herramientas de desarrollo.

CVE-2023-36792

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código en entornos de desarrollo/visualización de código.

Impacto en el Negocio:
Riesgo de interrupciones operativas y exposición de información si es explotado.

Acción Recomendada:
Parchear, revisar permisos de desarrollo y realizar pruebas de seguridad en entornos aislados antes de avanzar a producción.

DEMO

CVE-2023-36788

CVSS 7.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código en la pila .NET/Visual Studio.

Impacto en el Negocio:
Posible interrupción de servicios y exposición de datos si se explota.

Acción Recomendada:
Aplicar parches y validar en entornos de pruebas; reforzar controles de acceso y monitorear para detección temprana.

CVE-2019-1083

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo de DoS en la biblioteca CLR que podría degradar o bloquear servicios al procesar ciertas solicitudes web.

Impacto en el Negocio:
Podría causar interrupciones de servicios y afectar la disponibilidad de aplicaciones críticas, con impacto en operaciones y SLA.

Acción Recomendada:
Aplicar parches, endurecer configuraciones de servidor y realizar pruebas de carga para confirmar resiliencia. Monitorizar disponibilidad y métricas de rendimiento.

DEMO

CVE-2019-1006

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo de autenticación que podría permitir firmar tokens SAML con claves simétricas arbitrarias, permitiendo suplantación en algunas circunstancias.

Impacto en el Negocio:
Riesgo de acceso no autorizado a servicios protegidos, con potencial exposición de datos y desviación de procesos críticos.

Acción Recomendada:
Aplicar correcciones y auditar integraciones que utilicen WCF/WIF. Reforzar gestión de claves y monitorizar intentos de uso indebido de tokens.

CVE-2019-0981

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

DoS en .NET Framework y .NET Core debido al manejo inadecuado de ciertas solicitudes web.

Impacto en el Negocio:

Puede provocar caídas temporales de servicios y afectación de disponibilidad para usuarios finales.

Acción Recomendada:

Aplicar parche y revisar configuración de límites de recursos web. Realizar pruebas de resiliencia y monitoreo de tráfico para detectar picos anómalos.

DEMO

CVE-2019-0980

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

DoS en .NET Framework y .NET Core por manejo de solicitudes web inapropiado.

Impacto en el Negocio:

Interrupciones de servicios pueden impactar operaciones y cumplimiento de SLAs.

Acción Recomendada:

Instalar actualizaciones, ajustar límites de recursos y verificar estabilidad en entornos de prueba antes de pasar a producción.

CVE-2019-0820

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

DoS asociado al procesamiento de expresiones RegEx en .NET Framework y .NET Core.

Impacto en el Negocio:

Puede degradar rendimiento y disponibilidad de servicios críticos ante uso intensivo o entradas complejas.

Acción Recomendada:

Aplicar parches y revisar patrones de uso de RegEx en aplicaciones. Considerar limitaciones de tamaño de entradas y aplicar mitigaciones de seguridad.

DEMO

CVE-2020-1108

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?

DoS en .NET Core/Framework por manejo inapropiado de solicitudes web.

Impacto en el Negocio:

Puede causar interrupciones de servicios y afectación de disponibilidad para usuarios y clientes.

Acción Recomendada:

Parchear componentes afectados, endurecer configuración de servidor y monitorizar picos de tráfico para detectar ataques.

CVE-2021-24111

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework relacionada con manejo de entradas, que podría degradar servicios.

Impacto en el Negocio:
Riesgo de interrupciones en operaciones y afectación de experiencia de usuario en servicios afectados.

Acción Recomendada:
Aplicar parche y revisar configuraciones de límite de recursos. Ejecutar pruebas de estrés para validar resistencia tras la corrección.

DEMO

CVE-2022-21911

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework por manejo ineficiente de ciertas entradas o procesos.

Impacto en el Negocio:
Puede afectar la disponibilidad de servicios y la continuidad de operaciones, especialmente en picos de demanda.

Acción Recomendada:
Parchear y asegurar configuración de recursos. Realizar pruebas de resiliencia y vigilancia de logs para detectar explotación.

CVE-2022-26832

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework por vulnerabilidad de manejo de recursos.

Impacto en el Negocio:
Impacto en disponibilidad de servicios y capacidad de respuesta ante incidentes operativos.

Acción Recomendada:
Actualizar componentes, reforzar límites de recursos y monitorizar rendimiento para detectar intentos de afectación.

DEMO

CVE-2023-32030

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework/Visual Studio relacionado con operaciones de procesamiento.

Impacto en el Negocio:
Podría causar interrupciones en desarrollo y producción, afectando despliegues y servicio al cliente.

Acción Recomendada:
Aplicar parche y validar estabilidad en entornos de pruebas. Mantener vigilancia de incidencias y plan de contingencia para interrupciones rápidas.

CVE-2023-29331

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework/Visual Studio debido a manejo de ciertos procesos.

Impacto en el Negocio:
Podría interrumpir operaciones, afectar la capacidad de entrega de servicios y dañar la confianza de clientes.

Acción Recomendada:
Parchear, revisar flujos de trabajo que involucren Visual Studio y monitorizar para detectar esfuerzos de agotamiento de recursos.

DEMO

CVE-2023-24936

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Elevación de privilegios en .NET Framework/ASP.NET, permitiendo ganar permisos superiores.

Impacto en el Negocio:
Con permisos elevados, un atacante podría modificar configuraciones y acceder a datos sensibles, afectando continuidad y cumplimiento.

Acción Recomendada:
Aplicar parche, auditar y restringir privilegios de cuentas con acceso a componentes afectados, y realizar pruebas de escalamiento.

CVE-2024-21312

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Riesgo de ejecución remota de código en la pila .NET/Framework.

Impacto en el Negocio:
Podría permitir control no autorizado y afectar la disponibilidad y confidencialidad de datos.

Acción Recomendada:
Parchear y validar en entornos de prueba, monitorizar para detectar intentos de explotación y reforzar segmentación de red.

CVE-2024-29059

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Disposición de información sensible (Information Disclosure) en .NET Framework.

Impacto en el Negocio:
Filtración de datos podría exponer información sensible de clientes y operaciones, generando costos de mitigación y daño reputacional.

Acción Recomendada:
Aplicar parche y revisar configuraciones de acceso a datos. Implementar controles de cifrado y monitoreo de accesos anómalos.

DEMO

CVE-2024-43484

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework/Visual Studio.

Impacto en el Negocio:
Podría provocar interrupciones de servicios y afectar la disponibilidad de sistemas críticos.

Acción Recomendada:
Aplicar parche, reforzar gestión de recursos y plan de continuidad. Monitorear rendimiento y alertas de saturación.

DEMO

CVE-2024-43483

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework/Visual Studio.

Impacto en el Negocio:
Puede derivar en interrupciones de operaciones y reducción de productividad si se explota.

Acción Recomendada:
Parchear, validar compatibilidad y aplicar mitigaciones de carga. Supervisar servicios y realizar pruebas de resiliencia.

CVE-2026-33116

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Infinitas iteraciones/loop que causan DoS en .NET Framework.

Impacto en el Negocio:
Interrupciones de servicio y ralentización de procesos, afectando la continuidad operativa y experiencia de usuario.

Acción Recomendada:
Aplicar parche y revisar código/arquitectura para evitar bucles. Implementar defensas contra DoS y pruebas de carga para validar resiliencia.

DEMO

CVE-2026-23666

CVSS 7.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Fallo de validación de entradas que podría provocar DoS en la red.

Impacto en el Negocio:
Puede impedir operaciones, degradar rendimiento y afectar la disponibilidad de aplicaciones críticas.

Acción Recomendada:
Actualización de componentes y endurecimiento de validaciones de entrada. Realizar pruebas de seguridad y monitoreo de anomalías de red.

CVE-2024-21409

CVSS 7.3

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
RCE en .NET Framework/Visual Studio por procesamiento de entradas.

Impacto en el Negocio:
Control no autorizado sobre sistemas y posibles interrupciones de servicios, con impacto en operaciones y confidencialidad.

Acción Recomendada:
Parchear y validar en entornos de pruebas; reforzar monitoreo de seguridad y restringir acceso a entornos críticos.

DEMO

CVE-2024-38081

CVSS 7.3

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Elevación de privilegios en .NET Framework/Visual Studio.

Impacto en el Negocio:
Permite a terceros con acceso limitado escalar privilegios, afectando integridad y control de entornos.

Acción Recomendada:
Aplicar parche, auditar permisos y segmentar accesos a componentes críticos. Ejecutar pruebas de control de privilegios en un entorno seguro.

CVE-2023-36873

CVSS 5.9

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Spoofing en .NET Framework, permitiendo suplantación en ciertos procesos.

Impacto en el Negocio:
Puede permitir suplantación de identidad para acceder a sistemas o datos, dañando confianza y operaciones.

Acción Recomendada:
Aplicar parche y validar controles de autenticación y autorización. Reforzar monitoreo de accesos y realizar pruebas de simulación de suplantación.

DEMO

CVE-2026-32226

CVSS 5.9

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Race condition que puede provocar DoS al compartir recursos en .NET Framework.

Impacto en el Negocio:
Podría generar interrupciones de servicios y afectación de continuidad, especialmente en entornos con alta concurrencia.

Acción Recomendada:
Corregir condiciones de carrera, aplicar parche y reforzar sincronización de recursos. Ejecutar pruebas de estrés y monitorizar concurrencia.

CVE-2022-41064

CVSS 5.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Information Disclosure en .NET Framework.

Impacto en el Negocio:
Filtración de información sensible podría ocurrir, con implicaciones para clientes y operaciones internas.

Acción Recomendada:
Parchear, revisar configuraciones de acceso a datos y cifrado. Realizar revisión de logs y auditoría de accesos para detectar exposiciones.

CVE-2019-1142

CVSS 5.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Elevación de privilegios al permitir creación de archivos en ubicaciones arbitrarias.

Impacto en el Negocio:
Puede permitir persistencia no autorizada y manipulación de procesos críticos, afectando la integridad operativa.

Acción Recomendada:
Aplicar parche y endurecer políticas de creación de archivos. Revisar rutas de escritura y permisos de usuario con privilegios elevados.

DEMO

CVE-2019-0864

CVSS 5.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS por manejo de objetos en memoria heap en .NET Framework.

Impacto en el Negocio:
Riesgo de caídas de servicios y degradación de rendimiento, afectando continuidad y experiencia de clientes.

Acción Recomendada:
Parchear, optimizar manejo de memoria y monitorizar uso de heap. Realizar pruebas de resiliencia ante cargas realistas.

DEMO

CVE-2020-1476

CVSS 5.5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Elevación de privilegios al permitir acceso a archivos en caché en ASP.NET/.NET.

Impacto en el Negocio:
Potencial acceso no autorizado a información y cambios no deseados en aplicaciones; podría afectar operaciones críticas.

Acción Recomendada:
Parchear y revisar controles de caché y permisos. Limitar accesos a archivos en caché y validar integridad tras actualizaciones.

CVE-2023-21722

CVSS 5

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework/Visual Studio por manejo inadecuado de ciertas entradas.

Impacto en el Negocio:
Puede conducir a interrupciones de servicios y retrasos en procesos de negocio que dependen de estas herramientas.

Acción Recomendada:
Aplicar parche y validar disponibilidad de servicios. Realizar pruebas de carga y monitorear indicadores de rendimiento tras la corrección.

DEMO

CVE-2025-55248

CVSS 4.8

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Encriptación débil que podría exponer información sensible al ser transmitida en la red.

Impacto en el Negocio:
Riesgo de filtración de datos, afectar relaciones con clientes y cumplimiento normativo. Puede generar costos de respuesta ante incidentes.

Acción Recomendada:
Actualizar algoritmos y claves criptográficas a configuraciones seguras. Verificar transporte cifrado y realizar pruebas de penetración para validar robustez.

CVE-2020-16937

CVSS 4.7

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
Information Disclosure en memoria, permitiendo revelar contenidos de objetos en .NET Framework.

Impacto en el Negocio:
Filtraciones de datos podrían exponer información sensible a actores no autorizados, afectando la seguridad y la confianza.

Acción Recomendada:
Aplicar parche y revisar manejo de memoria. Implementar mitigaciones de exposición y monitorizar accesos a memoria.

DEMO

CVE-2022-30130

CVSS 3.3

Componente Afectado: .NET Framework (Microsoft)

¿Qué es esta vulnerabilidad?
DoS en .NET Framework por validación de entradas y procesamiento.

Impacto en el Negocio:
Podría ocasionar interrupciones de servicios y afectación de operaciones, especialmente en picos de demanda.

Acción Recomendada:
Parchear y revisar controles de validación. Realizar pruebas de carga y monitorizar para detectar posibles intentos de DoS.

Tabla Técnica Completa - Top 10 CVEs

CVE ID	CVSS	DESCRIPCIÓN TÉCNICA	COMPONENTE
CVE-2020-0646	9.8	Este tema podría permitir a un atacante remoto tomar control de un sistema si envía datos no válidos. La exposición de datos y la posibilidad de interrupciones podrían afectar operaciones críticas. Es importante aplicar parches y validar que las actualizaciones no impacten las operaciones diarias.	.NET Framework
CVE-2023-36049	9.8	Existe un riesgo de que alguien con cierto nivel de acceso obtenga más privilegios que los permitidos, cambiando configuraciones o datos. Esto podría afectar la seguridad de la plataforma y la continuidad de servicios. La acción clave es aplicar la corrección y revisar permisos de usuario.	.NET Framework
CVE-2024-0057	9.8	Un fallo podría permitir que controles de seguridad se bypassen, lo que podría facilitar acciones no autorizadas. Esto podría afectar la integridad de procesos y la confianza de los clientes. Se recomienda aplicar la corrección y reforzar las políticas de seguridad.	.NET Framework
CVE-2019-1113	8.8	Existe la posibilidad de que un atacante pueda ejecutar acciones de forma remota si se envían archivos con entradas problemáticas. Esto podría impactar servicios y secretos de la empresa. Es necesario aplicar el parche y validar entradas para evitar impactos.	.NET Framework
CVE-2020-0606	8.8	Hay un fallo que podría permitir tomar control del sistema si se procesan ciertas entradas. Esto podría afectar la disponibilidad y la seguridad de los datos. La acción recomendada es parchear y validar en pruebas antes de mantener en producción.	.NET Framework
CVE-2020-0605	8.8	Similar al caso anterior, existe riesgo de control no autorizado por manejo indebido de entradas. Esto podría impactar operaciones y confidencialidad de datos. Parchear y revisar controles de seguridad es clave.	.NET Framework
CVE-2023-36899	8.8	Un fallo podría permitir elevar privilegios dentro de la plataforma, facilitando cambios no autorizados. Esto puede afectar la seguridad, la integridad de los sistemas y las operaciones. Aplicar la corrección y auditar accesos es esencial.	.NET Framework

DEMO

CVE ID	CVSS	DESCRIPCIÓN TÉCNICA	COMPONENTE
CVE-2023-36560	8.8	Existe la posibilidad de omitir controles de seguridad, permitiendo acciones no autorizadas. El impacto puede incluir datos sensibles expuestos o cambios indeseados. La mitigación principal es aplicar el parche y revisar configuraciones de seguridad.	.NET Framework
CVE-2025-21176	8.8	Un fallo permitiría ejecutar código de forma remota y tomar control del sistema afectado. Eso podría derivar en pérdida de control, exposición de datos y interrupciones. La acción recomendada es parchear y vigilar posibles intentos de intrusión.	.NET Framework
CVE-2024-0056	8.7	Riesgo de acceso indebido a datos por evadir controles de seguridad en el proveedor de datos. Puede provocar exposición de información y afectar operaciones. Se recomienda parchear y revisar accesos a bases de datos.	.NET Framework
CVE-2020-1147	7.8	Existe la posibilidad de ejecución remota si se procesan entradas en XML de forma insegura. Esto podría afectar la continuidad y la confidencialidad de datos. Aplicar parche y validar entradas XML es crucial.	.NET Framework
CVE-2022-26929	7.8	Potencial ejecución remota de código, que podría permitir controlar sistemas y exponer datos. Esto impacta operación y fiabilidad. Es fundamental parchear y vigilar sistemas expuestos.	.NET Framework
CVE-2022-41089	7.8	Riesgo de ejecución remota de código que podría dar control del sistema. Frente a ello, la continuidad de servicios podría verse afectada. Se debe aplicar parche y monitorizar actividad.	.NET Framework
CVE-2023-21808	7.8	Existe posibilidad de ejecución remota de código en componentes afectados, con posible interrupción de servicios. La continuidad de operaciones podría verse comprometida. Parchear y validar en entornos de prueba es clave.	.NET Framework
CVE-2023-29326	7.8	Fallo que podría permitir ejecutar acciones no autorizadas y afectar la estabilidad de la plataforma. Esto podría impactar servicios y datos. Aplicar parche y verificar que las actualizaciones no interrumpan operaciones es esencial.	.NET Framework
CVE-2023-24897	7.8	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	.NET Framework

DEMO

CVE ID	CVSS	DESCRIPCIÓN TÉCNICA	COMPONENTE
CVE-2023-24895	7.8	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	.NET Framework
CVE-2023-36796	7.8	Visual Studio Remote Code Execution Vulnerability	.NET Framework
CVE-2023-36794	7.8	Visual Studio Remote Code Execution Vulnerability	.NET Framework
CVE-2023-36793	7.8	Visual Studio Remote Code Execution Vulnerability	.NET Framework
CVE-2023-36792	7.8	Visual Studio Remote Code Execution Vulnerability	.NET Framework
CVE-2023-36788	7.8	.NET Framework Remote Code Execution Vulnerability	.NET Framework
CVE-2019-1083	7.5	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests, aka '.NET Denial of Service Vulnerability'.	.NET Framework
CVE-2019-1006	7.5	An authentication bypass vulnerability exists in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAML tokens with arbitrary symmetric keys, aka 'WCF/WIF SAML Token Authentication Bypass Vulnerability'.	.NET Framework
CVE-2019-0981	7.5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0820, CVE-2019-0980.	.NET Framework
CVE-2019-0980	7.5	A denial of service vulnerability exists when .NET Framework or .NET Core improperly handle web requests, aka '.Net Framework and .Net Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0820, CVE-2019-0981.	.NET Framework
CVE-2019-0820	7.5	A denial of service vulnerability exists when .NET Framework and .NET Core improperly process RegEx strings, aka '.NET Framework and .NET Core Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0980, CVE-2019-0981.	.NET Framework

DEMO

CVE ID	CVSS	DESCRIPCIÓN TÉCNICA	COMPONENTE
CVE-2020-1108	7.5	A denial of service vulnerability exists when .NET Core or .NET Framework improperly handles web requests, aka '.NET Core & .NET Framework Denial of Service Vulnerability'.	.NET Framework
CVE-2021-24111	7.5	.NET Framework Denial of Service Vulnerability	.NET Framework
CVE-2022-21911	7.5	.NET Framework Denial of Service Vulnerability	.NET Framework
CVE-2022-26832	7.5	.NET Framework Denial of Service Vulnerability	.NET Framework
CVE-2023-32030	7.5	.NET and Visual Studio Denial of Service Vulnerability	.NET Framework
CVE-2023-29331	7.5	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	.NET Framework
CVE-2023-24936	7.5	Existe un riesgo de escalamiento de privilegios que podría permitir cambios no autorizados. Esto podría afectar la integridad y operación de sistemas. Aplicar parche y auditar permisos ayuda a mitigar.	.NET Framework
CVE-2024-21312	7.5	Fallo que podría permitir ejecutar código de forma remota y controlar sistemas. Esto impacta la disponibilidad y confidencialidad de la información. Parchear y monitorizar son acciones clave.	.NET Framework
CVE-2024-29059	7.5	Existe una posible divulgación de información sensible. Esto podría afectar a clientes y operaciones internas. Parchear, revisar permisos y cifrado ayuda a reducir riesgos.	.NET Framework
CVE-2024-43484	7.5	DoS que podría interrumpir servicios y afectar la disponibilidad. Operaciones y experiencia de usuario pueden verse comprometidas. Aplicar parche y vigilar rendimiento son medidas recomendadas.	.NET Framework
CVE-2024-43483	7.5	Riesgo de DoS que podría impactar la disponibilidad de servicios. Esto podría afectar entregas y satisfacción de clientes. Parchear y validar estabilidad es necesario.	.NET Framework

DEMO

CVE ID	CVSS	DESCRIPCIÓN TÉCNICA	COMPONENTE
CVE-2026-33116	7.5	Un bucle infinito podría provocar DoS y afectar la disponibilidad de la red. Operations y servicios podrían verse interrumpidos. Es clave aplicar parche y revisar código para evitar bucles.	.NET Framework
CVE-2026-23666	7.5	Entrada mal gestionada podría generar DoS en la red. Puede impactar la disponibilidad de aplicaciones críticas. Parchear y reforzar validaciones es la acción recomendada.	.NET Framework
CVE-2024-21409	7.3	Existe la posibilidad de ejecutar código de forma remota, con posible control de sistemas. Esto afecta la continuidad y confidencialidad. Parchear y monitorizar son medidas clave.	.NET Framework
CVE-2024-38081	7.3	Elevación de privilegios que podría permitir acciones no autorizadas. Esto pone en riesgo la seguridad de operaciones y datos. Aplicar parche y auditar accesos es fundamental.	.NET Framework
CVE-2023-36873	5.9	Posibilidad de suplantación de identidad en ciertos procesos. Esto podría permitir acceso indebido a sistemas. Parchear y fortalecer autenticación ayuda a mitigar.	.NET Framework
CVE-2026-32226	5.9	Condiciones de carrera podrían provocar DoS al compartir recursos. Esto podría interrumpir servicios y afectar productividad. Aplicar parches y revisar sincronización de recursos es recomendado.	.NET Framework
CVE-2022-41064	5.8	Filtración de información sensible podría ocurrir. Esto afecta clientes y operaciones internas. Parchear, revisar controles de datos y auditar accesos reduce el riesgo.	.NET Framework
CVE-2019-1142	5.5	Elevación de privilegios al permitir escritura de archivos en ubicaciones arbitrarias. Puede afectar integridad operativa. Parchear y revisar permisos de escritura es necesario.	.NET Framework
CVE-2019-0864	5.5	DoS por manejo de memoria en .NET Framework. Esto puede degradar rendimiento y disponibilidad. Aplicar parche y monitorear uso de memoria ayuda a mitigar.	.NET Framework
CVE-2020-1476	5.5	Elevación de privilegios a través de cachés. Puede permitir acceso no autorizado a información. Parchear y revisar caché/seguridad es crucial.	.NET Framework

DEMO

CVE ID	CVSS	DESCRIPCIÓN TÉCNICA	COMPONENTE
CVE-2023-21722	5	Riesgo de DoS por manejo de entradas en la pila .NET/Visual Studio. Esto puede afectar la disponibilidad de servicios y herramientas de desarrollo. Parchear y probar resiliencia es clave.	.NET Framework
CVE-2025-55248	4.8	Encriptación débil que podría exponer información durante la transmisión. Esto impacta la confidencialidad. Actualizar algoritmos y claves y asegurar transporte cifrado es fundamental.	.NET Framework
CVE-2020-16937	4.7	Filtración de información por manejo de memoria. Podría exponer contenidos sensibles. Parchear y revisar manejo de memoria reduce el riesgo.	.NET Framework
CVE-2022-30130	3.3	DoS por validación de entradas y procesamiento. Esto podría interrumpir servicios en momentos de alta demanda. Parchear y validar controles de entrada ayuda a mitigar.	.NET Framework

DEMO

Aplicaciones con Mayor Riesgo

Estas aplicaciones han sido identificadas como las más vulnerables del equipo. Se incluye el análisis de por qué representan un riesgo y qué acciones específicas se deben tomar.

APLICACIÓN	NIVEL DE RIESGO	ANÁLISIS Y RECOMENDACIONES
.NET Framework (Microsoft) *52 CVEs | CVSS Promedio: 7.42* #known_vulnerability #critical_vulnerability #easy_to_exploit #confidentiality_impact_if_exploited #exposed_to_credentials_stealing #exposed_to_sensitive_information_disclosure	RIESGO ALTO	**Por qué es riesgoso:** .NET Framework presenta una cantidad significativa de vulnerabilidades conocidas, con un alto puntaje de criticidad. Esto lo convierte en un objetivo atractivo para atacantes que buscan explotaciones a través de la ejecución remota de código o la divulgación de información sensible. **Acción: Aplicar actualizaciones de seguridad recomendadas por Microsoft y realizar auditorías periódicas para detectar vulnerabilidades potenciadas.**

Análisis de Vectores de Ataque

Análisis de Vectores de Ataque

Los x-tags sugieren una alta probabilidad de ataques de ejecución remota de código (RCE) y DoS, lo que podría comprometer la disponibilidad e integridad de los sistemas relacionados. Además, hay un riesgo significativo de robo de credenciales y divulgación de información sensible, lo que podría dañar la reputación y la confianza del negocio.

Tags Técnicos Detectados:

#known_vulnerability #critical_vulnerability #easy_to_exploit #confidentiality_impact_if_exploited #exposed_to_credentials_stealing #exposed_to_sensitive_information_disclosure #integrity_impact_if_exploited #availability_impact_if_exploited #exposed_to_DOS_Attack #exposed_to_RCE_attack #user_interaction_required_for_exploiting

¿Qué significan estos tags?

Los x-tags indican que .NET Framework está expuesto a varias vulnerabilidades críticas y fáciles de explotar. Estos tags ayudan a entender el riesgo de ataques que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos. La detección de vulnerabilidades conocidas y el posible requerimiento de interacción del usuario para la explotación son aspectos clave que deben ser considerados en la gestión de riesgos.

DEMO

Plan de Acción Priorizado

Recomendaciones organizadas por urgencia para remediar las vulnerabilidades identificadas. Priorice las

acciones críticas de esta semana para reducir inmediatamente la superficie de ataque.

ESTA SEMANA (Crítico)

- Realizar un análisis de las vulnerabilidades críticas asignando al equipo de TI una semana para generar un informe detallado.
- Desarrollar un protocolo de respuesta ante incidentes con el equipo de TI en un plazo de 5 días.
- Implementar medidas de mitigación inmediatas para las vulnerabilidades más críticas, encargado al equipo de TI, en el plazo de 3 días.

ESTE MES (Alto)

- Evaluar opciones de parches virtuales o soluciones temporales para aplicaciones vulnerables.
- Formar un plan de capacitación en ciberseguridad para el personal del equipo de TI.
- Revisar y actualizar las políticas de seguridad y gestión de vulnerabilidades.

PRÓXIMOS 3 MESES (Medio)

- Establecer un programa de monitoreo continuo de vulnerabilidades con herramientas adecuadas.
- Implementar un sistema de gestión de parches, cuando esté disponible, para las aplicaciones críticas.
- Realizar auditorías de ciberseguridad trimestrales para evaluar y mejorar la postura de seguridad.

DEMO

Recomendaciones Estratégicas

Medidas a largo plazo para mejorar la postura de seguridad general del equipo y prevenir futuras vulnerabilidades. Estas recomendaciones deben integrarse en la estrategia de ciberseguridad de la organización.

- ✓ Desarrollar un plan de respuesta a incidentes específico para vulnerabilidades críticas identificadas.
- ✓ Establecer un ciclo de revisión y actualización regular de las políticas de seguridad.
- ✓ Implementar controles de acceso estrictos para limitar la exposición de aplicaciones vulnerables.
- ✓ Asegurarse de que la estrategia de ciberseguridad esté alineada con la Ley 21.663 en cuanto a la gestión de riesgos y respuesta ante incidentes.

¿Necesita Ayuda Profesional?

Dado el alto riesgo asociado a las vulnerabilidades identificadas en su endpoint, es crucial actuar con urgencia para reducir la superficie de ataque y fortalecer la postura de seguridad. La Ley 21.663 promueve buenas prácticas de gestión de ciberseguridad y respuesta ante incidentes, orientadas a la prevención y mitigación de riesgos asociados a vulnerabilidades de seguridad.

Contáctenos: soporte@tecnoinver.cl

DEMO

Aviso de Confidencialidad

Este informe contiene análisis detallados de vulnerabilidades de infraestructura identificadas mediante el producto de Tecnoinver y un análisis avanzado con Inteligencia Artificial. Es estrictamente confidencial y está destinado únicamente a destinatarios autorizados. No debe divulgarse a terceros sin consentimiento por escrito de Tecnoinver. Los destinatarios son responsables de mantener su seguridad, garantizar su almacenamiento seguro y su eliminación adecuada. El uso no autorizado, la distribución o copia de este informe están prohibidos y pueden resultar en acciones legales.