Alerta Vulnerabilidad
Fallo Crítico de seguridad en ASP.NET

CSIRTSALUD-AV-202600423-42

TLP: CLEAR

Alerta ID:	042
Fecha del reporte:	23/04/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Fallo crítico de seguridad en ASP.NET
Herramienta de detección	N/A
Activo involucrado:	ASP.NET
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las entidades del ecosistema digital sobre la liberación de actualizaciones de seguridad de emergencia por parte de Microsoft, destinadas a corregir una vulnerabilidad crítica en ASP.NET Core. Esta vulnerabilidad, identificada como CVE-2026-40372, permite a los atacantes escalar privilegios y obtener acceso de sistema mediante la falsificación de cookies de autenticación. Las actualizaciones lanzadas son esenciales para evitar posibles explotaciones y garantizar la seguridad de las aplicaciones que utilizan ASP.NET Core en su infraestructura.

Descripción:

Microsoft ha lanzado actualizaciones de seguridad de emergencia para corregir una vulnerabilidad crítica en ASP.NET Core, identificada como CVE-2026-40372. Esta

vulnerabilidad afecta a las APIs criptográficas utilizadas por ASP.NET, específicamente en la protección de datos de autenticación. Los atacantes podrían aprovechar esta falla para falsificar cookies de autenticación, permitiéndoles escalar privilegios en el sistema y obtener acceso no autorizado con privilegios de administrador.

El fallo se encuentra en la validación de cookies durante el proceso de autenticación, lo que significa que un atacante podría enviar cookies modificadas para ganar acceso no autorizado a una aplicación web, sin necesidad de estar previamente autenticado. Esta vulnerabilidad es particularmente crítica debido a su impacto potencial, ya que permitiría a los atacantes realizar acciones administrativas y manipular los datos protegidos por la aplicación.

Las actualizaciones lanzadas por Microsoft abordan esta falla corrigiendo la validación de las cookies y reforzando la seguridad en las aplicaciones basadas en ASP.NET Core. La recomendación es aplicar las actualizaciones inmediatamente para mitigar el riesgo de explotación, ya que la vulnerabilidad ha sido clasificada como de alto riesgo y su explotación podría tener consecuencias graves para la seguridad y la privacidad de los usuarios y datos almacenados.

Consecuencias de la explotación

La explotación exitosa de la vulnerabilidad CVE-2026-40372 en ASP.NET Core puede tener graves consecuencias tanto a nivel técnico como operativo para las organizaciones afectadas. Entre las principales consecuencias se destacan las siguientes:

1. **Acceso no autorizado a sistemas administrativos**: Los atacantes que exploten esta vulnerabilidad podrían obtener privilegios de administrador en el sistema, lo que les

permitiría ejecutar comandos arbitrarios, modificar configuraciones críticas y acceder a información sensible almacenada en las aplicaciones afectadas.

2. **Escalamiento de privilegios**: Al falsificar cookies de autenticación, los atacantes podrían escalar privilegios dentro de la aplicación o el servidor, lo que les permitiría tomar control completo sobre los sistemas afectados.
3. **Manipulación de datos sensibles**: Con acceso de administrador, los atacantes tendrían la capacidad de modificar, eliminar o robar datos confidenciales, lo que podría incluir información personal, financiera o de clientes. Esto podría resultar en violaciones de privacidad y potenciales demandas por incumplimiento de normativas de protección de datos.
4. **Compromiso de la infraestructura de TI**: La explotación de esta vulnerabilidad podría extenderse a otros sistemas interconectados dentro de la infraestructura de TI de la organización, permitiendo el movimiento lateral y el acceso a sistemas críticos, como bases de datos, servidores y redes internas.
5. **Riesgos reputacionales**: El compromiso de datos sensibles y la falta de respuesta ante un ataque exitoso podría causar daños a la reputación de la organización, afectando la confianza de los clientes, socios y reguladores.
6. **Impacto regulatorio**: Las organizaciones que manejen información personal o confidencial podrían enfrentar sanciones bajo regulaciones como el Reglamento General de Protección de Datos (GDPR) en Europa, o la Ley 1581 de 2012 en Colombia, debido a la exposición de datos sensibles sin las protecciones adecuadas.

Modo de explotación del ataque

La explotación de la vulnerabilidad CVE-2026-40372 en ASP.NET Core puede llevarse a cabo mediante las siguientes fases claramente definidas:

Fase 1 – Identificación y manipulación de cookies de autenticación

El ataque comienza cuando el atacante identifica una aplicación web vulnerable que utiliza ASP.NET Core y la vulnerabilidad en la validación de cookies. Utilizando técnicas de manipulación, el atacante falsifica cookies de autenticación legítimas y las envía al servidor para su procesamiento.

Fase 2 – Escalamiento de privilegios mediante cookies falsas

Una vez que las cookies falsas son aceptadas por la aplicación web, el atacante puede escalar privilegios dentro de la aplicación, eludiendo la necesidad de autenticación. Esto le permite obtener acceso administrativo o incluso ejecutar acciones no autorizadas en el servidor.

Fase 3 – Acceso no autorizado a datos y comandos remotos

Con privilegios elevados, el atacante puede acceder y manipular información sensible almacenada en la aplicación web. Además, podría ejecutar comandos arbitrarios en el servidor afectado, comprometiendo así la integridad y la seguridad de la infraestructura de TI.

Fase 4 – Persistencia y evasión

El atacante puede intentar establecer persistencia en el sistema afectado, manteniendo su acceso a través de configuraciones modificadas o backdoors. Al ser capaz de eludir la detección

de las soluciones de seguridad, el atacante puede operar de manera oculta durante períodos prolongados.

Vulnerabilidades asociadas

- La vulnerabilidad CVE-2026-40372 en ASP.NET Core no depende de la explotación de un fallo específico en el software, sino que se origina en una debilidad inherente en la validación de cookies de autenticación. Sin embargo, su explotación puede aprovechar las siguientes características de seguridad mal gestionadas:
- Falla en la validación de cookies: La vulnerabilidad se debe a un defecto en la validación de cookies en el sistema de autenticación de ASP.NET Core, que permite que un atacante falsifique cookies y las utilice para ganar acceso no autorizado a la aplicación web. Este defecto compromete la integridad del proceso de autenticación, permitiendo que los atacantes puedan actuar como usuarios autenticados.
- Uso inseguro de mecanismos de autenticación: La vulnerabilidad también resalta la importancia de implementar mecanismos de autenticación robustos y controles de validación adicionales. La falta de validación adecuada de los tokens de autenticación y las cookies pone en riesgo a las aplicaciones, permitiendo a los atacantes acceder a las funciones de la aplicación como si fueran usuarios privilegiados.
- Exposición de datos sensibles sin cifrado: La vulnerabilidad podría ser más peligrosa si se combina con malas prácticas de manejo de datos sensibles. Si los datos de autenticación no están debidamente cifrados o si las cookies pueden ser manipuladas fácilmente, el riesgo de exfiltración de información sensible aumenta.

- Falta de control de acceso adecuado: La vulnerabilidad también refleja una falta de control de acceso estricto, permitiendo que un atacante con cookies falsas pueda escalar privilegios sin autenticarse completamente o sin ser verificado correctamente. La ausencia de medidas de seguridad como Multi-Factor Authentication (MFA) puede agravar este problema.

Recomendaciones de detección y mitigación

Los equipos de seguridad, infraestructura y desarrollo deben priorizar la actualización inmediata de todos los entornos afectados hacia la versión corregida del framework y del runtime correspondiente. Microsoft ya publicó .NET 10.0.7 y ASP.NET Core Runtime 10.0.7, por lo que se recomienda verificar servidores, contenedores, imágenes base, pipelines de despliegue y componentes de hospedaje para asegurar que no permanezcan instancias desactualizadas en producción, pruebas o contingencia.

Adicionalmente, se recomienda realizar un inventario técnico de todas las aplicaciones que utilicen autenticación basada en cookies y mecanismos de ASP.NET Core Data Protection, dado que este subsistema es el encargado de proteger y validar información sensible como cookies y otros datos confiables enviados al cliente. Este ejercicio debe incluir la identificación del repositorio del key ring, el esquema de despliegue en múltiples nodos y las cuentas de servicio con acceso a dicho repositorio.

Entre las medidas prioritarias se recomienda aplicar las siguientes:

1. Actualizar de forma prioritaria todos los runtimes y componentes de hospedaje de ASP.NET Core en servidores Windows, Linux, macOS y contenedores donde existan aplicaciones expuestas o internas que dependan de autenticación por cookies.

2. Proteger estrictamente el almacenamiento del key ring. Microsoft indica que el repositorio de claves de Data Protection debe limitarse únicamente a la identidad bajo la cual corre la aplicación, con permisos de lectura, escritura y creación solo para esa cuenta. Esto aplica tanto a almacenamiento en disco como a Blob Storage u otros repositorios compartidos.
3. Revisar el ciclo de vida, rotación y revocación de claves. El sistema de Data Protection gestiona automáticamente la vida útil de las claves; por defecto, crea y rota claves con una lógica de expiración y activación definida. Si existe sospecha de exposición o abuso, puede revocarse el key ring y generarse una nueva clave, lo que además invalida la caché en memoria en la siguiente operación de protección o desprotección.
4. Evitar la eliminación manual de claves como mecanismo improvisado de respuesta. La documentación oficial advierte que borrar una clave del key ring vuelve permanentemente indescifrables los datos protegidos con ella. En escenarios de respuesta, la acción correcta es revocar y rotar, no eliminar sin control.
5. Fortalecer la instrumentación de autenticación y el registro de eventos. ASP.NET Core dispone de logging estructurado mediante ILogger y permite suscribirse a eventos de autenticación por cookie. Como medida de detección derivada de esa arquitectura, conviene registrar y alertar sobre inicios de sesión atípicos, renovaciones inusuales de cookie, cambios inesperados de privilegios, respuestas 401/403 anómalas y patrones de autenticación administrativa fuera de horario o desde orígenes no habituales.
6. Revisar la configuración de endurecimiento de cookies en las aplicaciones, incluyendo atributos como HttpOnly, Secure y SameSite, para reducir superficie de abuso y asegurar que la emisión de cookies siga prácticas seguras acordes con el flujo de autenticación implementado.

7. Validar la configuración de Data Protection en despliegues distribuidos. Microsoft señala que cuando una aplicación está desplegada en múltiples máquinas o entornos, debe configurarse de forma explícita el sistema de Data Protection y proteger adecuadamente el mecanismo de almacenamiento de claves, ya que de ello depende la integridad del proceso criptográfico asociado a cookies y otros datos confiables

Recomendaciones de prevención y mitigación

Para prevenir la explotación de la vulnerabilidad CVE-2026-40372 y fortalecer la seguridad de las aplicaciones que utilizan ASP.NET Core, se recomienda implementar las siguientes medidas de prevención y fortalecimiento:

1. **Aplicar las actualizaciones de seguridad de inmediato**: Las actualizaciones de emergencia de .NET 10.0.7 y ASP.NET Core Runtime 10.0.7 deben ser aplicadas en todos los entornos afectados, incluidas servidores y contenedores que hospeden aplicaciones basadas en ASP.NET Core. Asegúrese de que tanto los runtimes como las aplicaciones estén actualizados a la última versión disponible.
2. **Fortalecer la protección de cookies de autenticación**: Utilice atributos de seguridad adicionales para las cookies, tales como HttpOnly, Secure y SameSite, para restringir el acceso y evitar que los atacantes roben o manipulen cookies de autenticación. Asegúrese de que la configuración de cookies se ajuste a las mejores prácticas recomendadas para ASP.NET Core.
3. **Implementar autenticación multifactor (MFA)**: La activación de MFA (autenticación multifactor) es una medida efectiva para reducir el riesgo de acceso no autorizado, incluso si un atacante logra falsificar una cookie de autenticación. Esto agrega una capa adicional de protección para las aplicaciones críticas que utilizan ASP.NET Core para la autenticación de usuarios.

4. **Revisar y proteger el repositorio de claves de Data Protection**: Asegúrese de que el repositorio de claves de Data Protection esté configurado correctamente y restringido a las identidades adecuadas. El acceso debe ser controlado mediante políticas de acceso estrictas, limitando su lectura y escritura solo a las cuentas de servicio necesarias. Evite almacenar las claves de manera no cifrada o en ubicaciones accesibles para usuarios no autorizados.
5. **Rotación y revocación periódica de claves**: Implemente políticas de rotación periódica de claves dentro de Data Protection, y revocar las claves comprometidas de manera inmediata si hay sospechas de que han sido filtradas o expuestas. Establezca un procedimiento para la revocación de cookies en caso de incidentes de seguridad.
6. **Monitoreo de autenticación y registro de eventos**: Implemente un sistema de registro detallado para todas las operaciones de autenticación y autorización en las aplicaciones que utilizan ASP.NET Core. Asegúrese de que los registros incluyan detalles sobre intentos de inicio de sesión, cambios en los privilegios y cualquier anomalía en las cookies de autenticación. Configure alertas para detectar patrones sospechosos, como intentos de acceso sin credenciales válidas.
7. **Evaluación de vulnerabilidades en las aplicaciones web**: Realice evaluaciones de seguridad periódicas a las aplicaciones que utilicen ASP.NET Core para identificar posibles vulnerabilidades y puntos débiles en la implementación de seguridad. Utilice herramientas automatizadas de escaneo de seguridad web, junto con revisiones manuales, para asegurarse de que la aplicación esté protegida frente a otros vectores de ataque.
8. **Implementar un enfoque de defensa en profundidad**: Asegúrese de que las aplicaciones cuenten con múltiples capas de seguridad, incluyendo firewall, inspección de tráfico y control de acceso, para mitigar el impacto de la explotación de cualquier

vulnerabilidad. Además, promueva prácticas de codificación segura durante el ciclo de vida del desarrollo para prevenir vulnerabilidades futuras.

Recomendaciones de respuesta ante compromiso

En caso de que se confirme un compromiso debido a la explotación de la vulnerabilidad CVE-2026-40372 en ASP.NET Core, se deben seguir los siguientes pasos para contener el incidente, mitigar el daño y restaurar la seguridad de los sistemas afectados:

1. **Aislamiento de los sistemas comprometidos**: Desconectar inmediatamente los servidores y aplicaciones afectados de la red para evitar que la vulnerabilidad se propague o que los atacantes mantengan el acceso no autorizado. Si el compromiso es global, considerar la desconexión temporal de todos los entornos de ASP.NET Core afectados.
2. **Aplicación de actualizaciones de seguridad**: Aplicar de forma urgente las actualizaciones de seguridad recomendadas por Microsoft, es decir, .NET 10.0.7 y ASP.NET Core Runtime 10.0.7, a todas las instancias afectadas. Asegúrese de que todas las aplicaciones en producción, desarrollo y prueba estén actualizadas.
3. **Revisión y revocación de cookies comprometidas**: Revocar todas las cookies de autenticación potencialmente comprometidas. Realice un barrido de los sistemas para detectar cualquier cookie falsificada y elimine cualquier token de autenticación válido que pueda haber sido manipulado por los atacantes.
4. **Auditoría de registros y actividades**: Realizar una auditoría exhaustiva de los registros de autenticación y otras actividades relacionadas con el sistema afectado. Revise cualquier anomalía en los intentos de inicio de sesión, escalado de privilegios y acciones administrativas, y monitoree los registros para detectar accesos no autorizados.

5. **Restablecimiento de credenciales**: Restablecer todas las credenciales de las cuentas de usuario y administrador involucradas en el sistema comprometido. Asegúrese de que las contraseñas se cambien de inmediato, especialmente para las cuentas con privilegios elevados.
6. **Análisis forense de la infraestructura afectada**: Realice un análisis forense completo para determinar el alcance del ataque y obtener evidencia de la explotación de la vulnerabilidad. Esto incluye la captura de imágenes de disco de los sistemas comprometidos, la recopilación de logs y la verificación de los repositorios de claves para asegurar que no haya otras brechas.
7. **Restauración desde copias seguras**: En caso de que se haya confirmado la manipulación de datos o la instalación de malware, considere restaurar el sistema desde copias de seguridad verificadas que no se hayan visto comprometidas. Asegúrese de que las copias de seguridad estén libres de vulnerabilidades y actualizadas con los últimos parches de seguridad.
8. **Notificación y reporte**: Notificar el incidente a las autoridades competentes, como CSIRT o el equipo de respuesta ante incidentes de la organización. Si el compromiso involucra datos sensibles, como información personal de clientes o usuarios, se debe cumplir con las regulaciones de privacidad correspondientes, como la Ley 1581 de 2012 (Protección de Datos Personales) en Colombia o el GDPR en Europa.
9. **Comunicaciones con los usuarios y clientes**: Si los datos de los usuarios se han visto comprometidos, es fundamental informar a los afectados de manera clara y transparente sobre el incidente, las medidas adoptadas y los pasos que deben seguir para protegerse. Proporcione orientación sobre cómo monitorear cuentas y establecer alertas de seguridad.

10. **Revisión de medidas de seguridad**: Después de mitigar el incidente, realice una revisión completa de la infraestructura de seguridad de las aplicaciones afectadas. Asegúrese de que las medidas de autenticación sean lo suficientemente robustas para prevenir futuros ataques, y considere la implementación de autenticación multifactor (MFA) si no se había adoptado previamente.

Conclusiones

La vulnerabilidad CVE-2026-40372 en ASP.NET Core representa un riesgo significativo para las organizaciones que dependen de este framework para la autenticación y protección de datos. La explotación exitosa de esta vulnerabilidad permite a los atacantes escalar privilegios y obtener acceso no autorizado a sistemas y datos sensibles, lo que podría tener un impacto devastador tanto a nivel operativo como reputacional.

Las medidas de prevención, como la aplicación inmediata de las actualizaciones de seguridad proporcionadas por Microsoft, la protección reforzada de las cookies de autenticación, y la rotación de claves de Data Protection, son fundamentales para mitigar el riesgo de explotación. Además, la implementación de autenticación multifactor (MFA) y la auditoría de registros fortalecerán las defensas contra ataques futuros.

Es crucial que las organizaciones respondan rápidamente ante cualquier indicio de explotación de esta vulnerabilidad, siguiendo los procedimientos de contención, mitigación y recuperación establecidos, para minimizar el impacto y restaurar la seguridad de sus sistemas afectados.

Este incidente subraya la importancia de mantener las aplicaciones actualizadas, realizar auditorías de seguridad periódicas y adoptar una estrategia de defensa en profundidad para proteger los datos y sistemas frente a amenazas cada vez más sofisticadas.

Fuentes:

- **Microsoft Security Response Center (MSRC)** – *Microsoft releases emergency security updates for critical ASP.NET flaw*. Disponible en: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-40372
- **BleepingComputer** – *Microsoft releases emergency security updates for critical ASP.NET flaw*. Disponible en: https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-security-updates-for-critical-aspnet-flaw/
- **dotnet.microsoft.com** – *Download .NET Core*. Disponible en: https://dotnet.microsoft.com/es-es/download/dotnet/10.0

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.