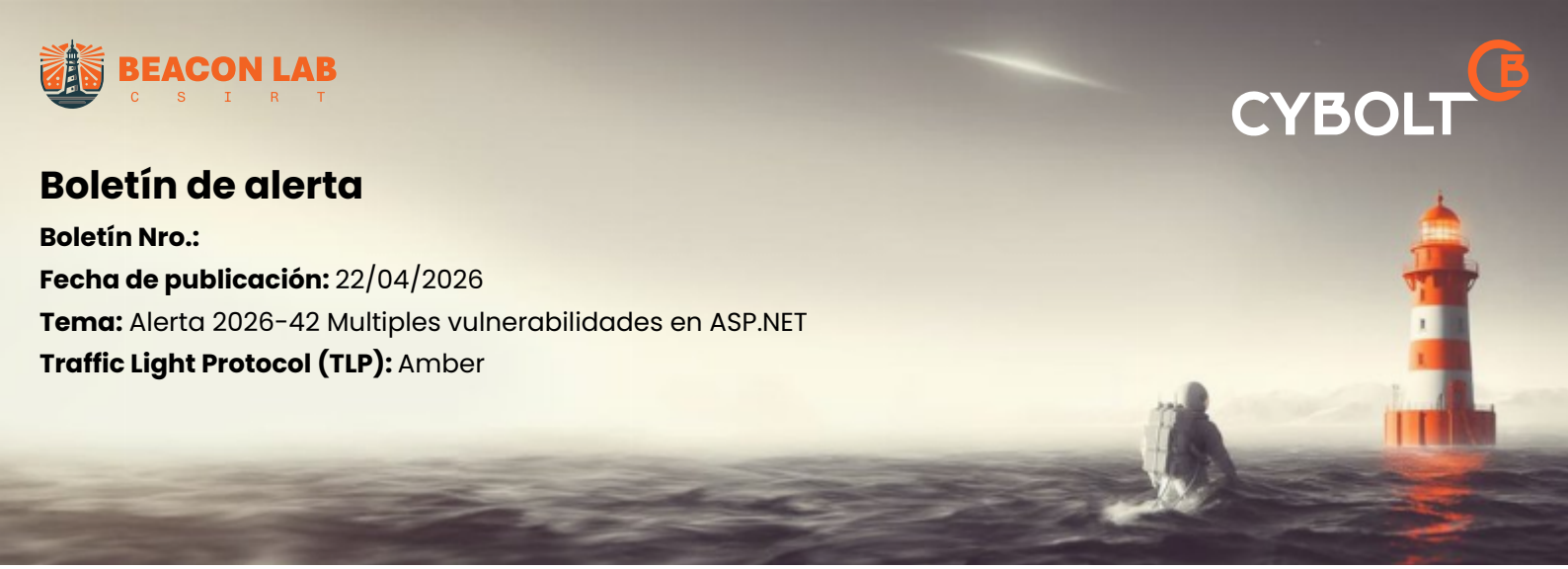

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 22/04/2026
Tema: Alerta 2026-42 Multiples vulnerabilidades en ASP.NET
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- ASP.NET Core (paquete **Microsoft.AspNetCore.DataProtection**) versiones 10.0.0 a 10.0.6, incluyendo aplicaciones que usan el runtime .NET 10.0.6 con ese componente

Descripción

Se ha identificado una vulnerabilidad crítica (CVSS 9.1) catalogada como CVE-2026-40372, la cual podría permitir a un atacante comprometer sistemas vulnerables dependiendo de la configuración y exposición del servicio afectado.

Esta vulnerabilidad está asociada a una debilidad en la validación de entradas y/o manejo de componentes internos, lo que podría ser explotado para ejecutar acciones no autorizadas dentro del sistema.

En escenarios de explotación exitosa, un atacante podría ejecutar código arbitrario en el sistema afectado, acceder a información sensible, escalar privilegios dentro del entorno comprometido y alterar la integridad del sistema o de los servicios asociados.

El riesgo se incrementa significativamente en entornos donde los servicios vulnerables están expuestos a Internet, existen accesos remotos sin controles robustos, no se cuenta con una segmentación de red adecuada o los sistemas no han sido actualizados o parcheados oportunamente.

Solución y mitigaciones:

Se recomienda implementar de forma inmediata, como mínimo, la aplicación de los parches de seguridad y actualizaciones proporcionadas por el fabricante para CVE-2026-33826, siguiendo la guía oficial de Microsoft: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33826. En paralelo, es aconsejable reforzar los controles de acceso al servicio afectado (segmentación de red, listas de control de acceso, uso de VPN para accesos administrativos) y asegurar que las cuentas con privilegios elevados utilicen autenticación multifactor (MFA).

Adicionalmente, en entornos donde existan indicios de explotación o alta exposición, se recomienda considerar medidas de respuesta reforzada como la rotación de credenciales sensibles (incluidas claves API y tokens), la invalidación de sesiones activas con exigencia de nueva autenticación, el endurecimiento de políticas de acceso remoto conforme al principio de mínimo privilegio y la monitorización intensiva de registros de autenticación y actividad administrativa para detectar posibles escaladas de privilegios o movimientos laterales no autorizados.

Información adicional:

- https://thehackernews.com/2026/04/microsoft-patches-critical-aspnet-core.html
- https://nvd.nist.gov/vuln/detail/CVE-2026-40372
- https://www.esecurityplanet.com/threats/cve-2026-40372-microsoft-patches-asp-net-core-privilege-escalation-vulnerability/
- https://devblogs.microsoft.com/dotnet/dotnet-10-0-7-oob-security-update/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-security-updates-for-critical-aspnet-flaw/