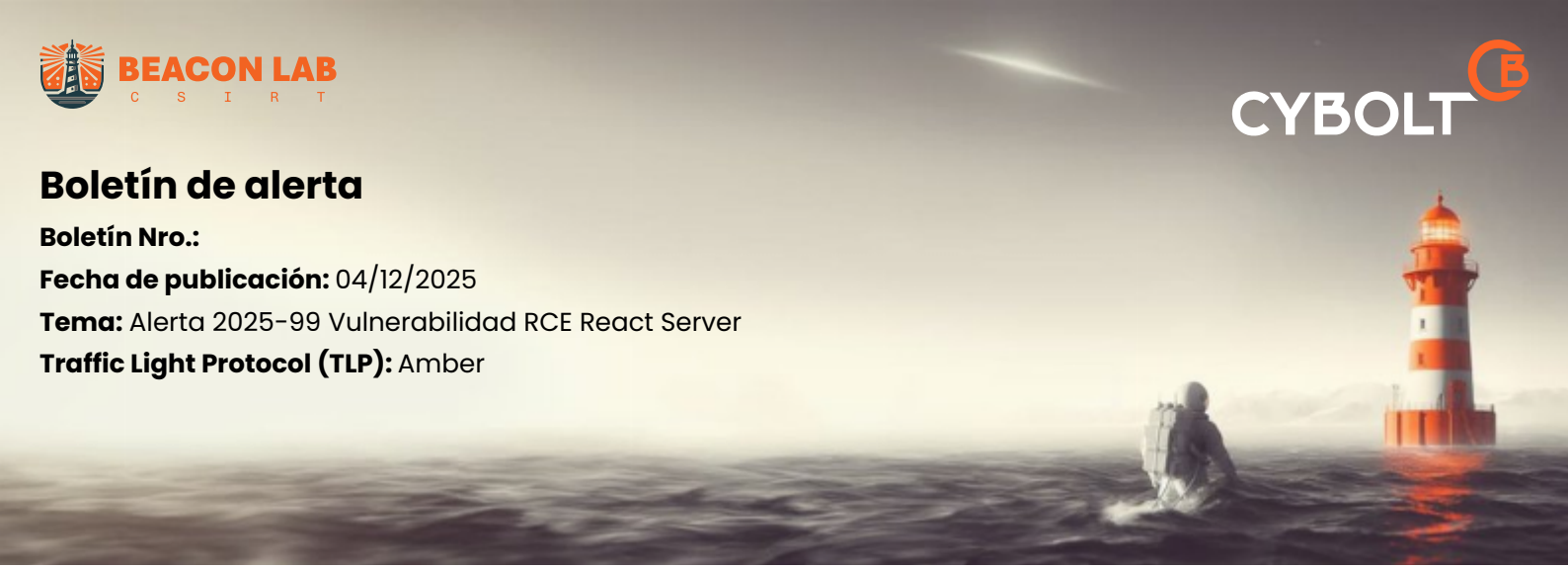

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 04/12/2025
Tema: Alerta 2025-99 Vulnerabilidad RCE React Server
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- React Server versions 19.0, 19.1.0, 19.1.1 y 19.2.0

Descripción

Se ha encontrado una vulnerabilidad crítica en React, una librería para interfaces de usuario web y nativas, que crea interfaces de usuario a partir de componentes individuales escritos en JavaScript. La misma ha sido catalogada como CVE-2025-55182 y permite la ejecución remota de código (RCE) previa a la autenticación en aplicaciones que utilizan React Server Components (RSC).

El problema está relacionado con una deserialización insegura puesto que cuando React o un framework que lo use procesa payloads, los interpreta sin validarlos correctamente, permitiendo que un atacante controle la ejecución en el servidor. La vulnerabilidad existe en configuraciones por defecto, por lo que muchas aplicaciones creadas con los métodos estándar serían vulnerables sin necesidad de modificaciones extra.

Cuando un usuario activa una acción del servidor, como hacer clic en un botón, el navegador inicia una solicitud POST para que Flight Server la procese. Su función principal consiste en recibir el cuerpo de la solicitud HTTP entrante y deserializar ese texto sin procesar en objetos JavaScript utilizables para que sirvan como argumentos de la función.

Una vez descomprimidos los datos, el servidor utiliza un formato de identificador basado en cadenas para asignar las referencias del cliente al código del servidor, con el formato ManifestID#ExportName. Finalmente, ejecuta la función JavaScript correspondiente.

Cuando un usuario activa una acción del servidor, como hacer clic en un botón, el navegador inicia una solicitud POST para que el servidor Flight la procese. Su función principal consiste en recibir el cuerpo de la solicitud HTTP entrante y deserializar ese texto sin formato en objetos JavaScript utilizables, que sirven como argumentos de función.

En esencia, se trata de una vulnerabilidad de deserialización insegura, derivada de un error lógico en la decodificación del protocolo «Flight» personalizado de React en el servidor.

La vulnerabilidad reside en la función requireModule del paquete react-server-dom-webpack. Esta función se encarga de resolver y cargar las funciones exportadas que un cliente intenta llamar en el servidor.

En JavaScript, acceder a una propiedad mediante la notación de corchetes (obj[key]) no solo comprueba las propiedades del objeto, sino que recorre toda la cadena del prototipo. El código no valida que el nombre de la exportación solicitada sea una exportación legítima, definida por el desarrollador.

Mitigación:

- Implementar reglas de Firewall de aplicaciones web (WAF) si están disponibles
- Aplicar las correcciones de las versiones 19.0.1, 19.1.2, or 19.2.1
- Monitorear el tráfico HTTP a los puntos finales de la función del servidor para detectar cualquier solicitud sospechosa o malformada
- Considerar restringir temporalmente el acceso a la red a las aplicaciones afectadas

Información adicional:

- https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
- https://my.f5.com/manage/s/article/K000158058
- https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerability-in-react-server-components-cve-2025-55182
- https://www.cve.org/CVERecord?id=CVE-2025-55182
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/ejecucion-remota-de-codigo-en-react-server-components?sstc=u88504nl590989
- https://securityonline.info/catastrophic-react-flaw-cve-2025-55182-cvss-10-0-allows-unauthenticated-rce-on-next-js-and-server-components/