Boletín informativo
Vulnerabilidad React2Shell

CSIRTSALUD-AV-20251212-17 **TLP: CLEAR**

Incidente ID:	0017
Fecha del reporte:	11/12/2025
Entidad:	Ecosistema Digital
Título:	Vulnerabilidad crítica React2Shell
Herramienta de detección	N/A
Activo involucrado:	N/A
Tipo de incidente:	Boletín informativo
Nivel de riesgo:	Alto

Objetivo:

Informar a las Entidades del Ecosistema Digital sobre la vulnerabilidad crítica de explotación activa CVE-2025-55182 (*React2Shell*), que afecta componentes del framework de desarrollo React y puede permitir la ejecución remota de código no autenticada.

Descripción:

Se identificó la vulnerabilidad crítica CVE-2025-55182, conocida como React2Shell, la cual está siendo explotada activamente según lo reportado en el catálogo CISA Known Exploited Vulnerabilities (KEV). Esta falla afecta a aplicaciones desarrolladas con React Server Components y permite la ejecución remota de código (RCE) sin requerir autenticación, lo que la clasifica con una severidad máxima (CVSS 10.0).

De acuerdo con reportes de The Hacker News y otras fuentes especializadas, actores maliciosos incluyendo grupos avanzados (APT) asociados a China y Corea del Norte están explotando esta vulnerabilidad en ataques reales, comprometiendo servidores web y desplegando malware como EtherRAT. Se estima que más de 70.000 sistemas expuestos públicamente podrían estar vulnerables, con decenas de organizaciones ya afectadas por campañas de explotación activa.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Productos afectados:

Las siguientes versiones de los paquetes que implementan React Server Components (RSC) contienen la vulnerabilidad CVE-2025-55182:

Paquetes React afectados	Versiones vulnerables
react-server-dom-webpack	19.0, 19.1.0, 19.1.1, 19.2.0
react-server-dom-parcel	19.0, 19.1.0, 19.1.1, 19.2.0
react-server-dom-turbopack	19.0, 19.1.0, 19.1.1, 19.2.0

Aunque la vulnerabilidad original está en React Server Components, Next.js queda afectado debido a su dependencia de RSC, y tiene sus propias versiones vulnerables que se correlacionan con CVE-2025-66478 (considerado duplicado de CVE-2025-55182):

Next.js vulnerable
Versiones 15.0.0 hasta 15.5.6
Versiones 16.0.0 hasta 16.0.6
Canary 14 después de 14.3.0-canary.76

Modo de explotación

La vulnerabilidad React2Shell (CVE-2025-55182) es una ejecución remota de código (RCE) sin necesidad de autenticación causada por una deserialización insegura dentro del protocolo Flight usado por React Server Components (RSC).

Como se explota:

1. **Envío de una solicitud HTTP maliciosa**

Un atacante envía una solicitud HTTP específicamente diseñada a un endpoint del servidor que procesa React Server Components. Esta petición contiene una carga útil (payload) manipulada que el servidor intenta deserializar.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

2. **Procesamiento inseguro de la deserialización**

El servidor interpreta datos estructurados del protocolo Flight sin realizar la validación adecuada, lo que permite que datos controlados por el atacante modifiquen objetos internos (incluyendo la contaminación de prototipos en JavaScript).

3. **Inyección de código arbitrario**

Debido a la deserialización insegura, el atacante puede forzar la ejecución de funciones peligrosas en el servidor, hasta ejecutar código JavaScript arbitrario o comandos del sistema. Esta ejecución remota puede, por ejemplo, iniciar procesos, descargar malware o abrir backdoors.

4. **Acceso como RCE sin credenciales**

El ataque no requiere autenticación ni privilegios previos; basta con que la aplicación acepte y procese el payload vulnerable.

Nota importante

En fuentes abiertas ya se encuentran disponibles diversas pruebas de concepto (PoC) para la explotación de la vulnerabilidad CVE-2025-55182, conocida como React2Shell, incluyendo payloads que aprovechan la deserialización insegura en React Server Components y herramientas que permiten validar y reproducir el comportamiento descrito en los reportes oficiales. Plataformas como GitHub y laboratorios de investigación independientes han publicado PoC funcionales que demuestran cómo una solicitud HTTP manipulada puede desencadenar ejecución remota de código (RCE) sin autenticación, facilitando la verificación de sistemas vulnerables. La disponibilidad pública de estas PoC incrementa significativamente la probabilidad de que actores maliciosos adopten rápidamente estos métodos en nuevas campañas de explotación.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

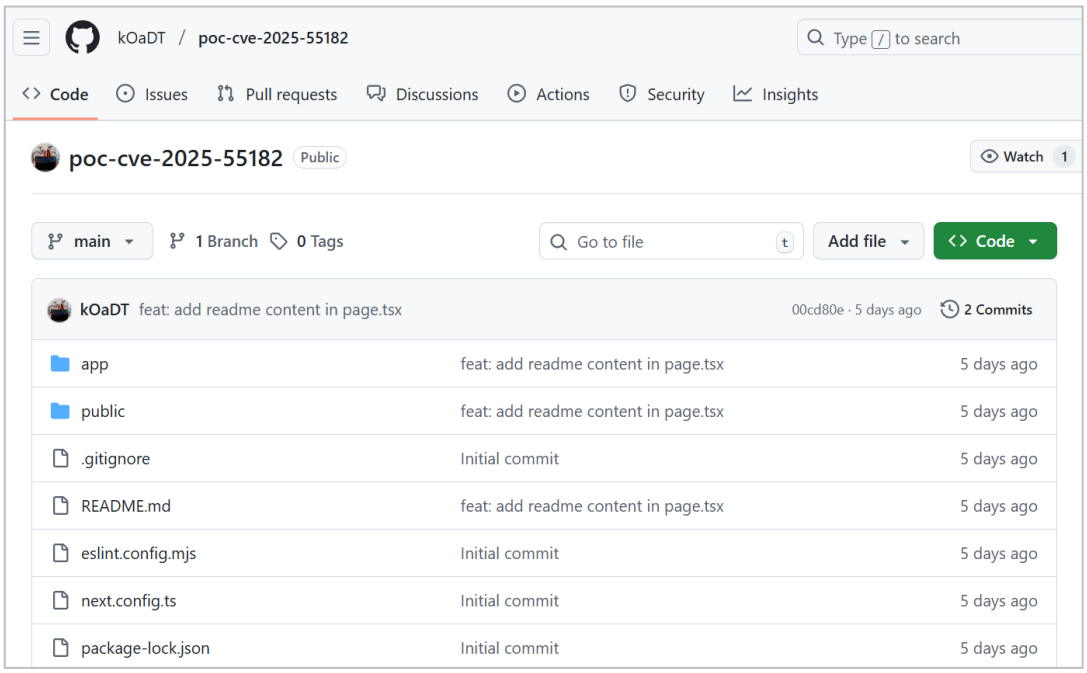

Ilustración 1.Poc Github

Fuente: Elaboración propia CSIRT Salud

Técnicas MITRE ATT&CK Detectadas:

ID	Técnica	Descripción
T1134.001	Access Token Manipulation	React2Shell puede permitir que los atacantes ejecuten código en el contexto del servidor, lo cual abre la puerta a robar o manipular tokens en memoria.
T1190	Exploit Public-Facing Application	React2Shell se explota mediante una petición HTTP maliciosa contra un servicio web expuesto
T1059	Command and Scripting Interpreter	Una vez obtenida RCE, atacantes ejecutan comandos en el servidor
T1203	Exploitation for Client Execution	La falla fuerza al servidor a ejecutar código en su propio contexto.
T1105	Ingress Tool Transfer	Reportes indican que se ha usado React2Shell para descargar malware como EtherRAT.
T1027	Obfuscated/Encrypted Files or Information	Muchos PoC usan payloads ofuscados dentro del protocolo Flight para evadir detección.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Recomendaciones de mitigación:

- Aplicar de inmediato las actualizaciones oficiales publicadas por react, instalando las versiones corregidas que eliminan la vulnerabilidad y reducen completamente el vector de explotación identificado.

  A continuación, se presentan las versiones vulnerables de react y su respectiva actualización para corregir la vulnerabilidad.

Paquetes React afectados	Versiones vulnerables	Versiones corregidas
react-server-dom-webpack	19.0, 19.1.0, 19.1.1, 19.2.0	19.0.1, 19.1.2, 19.2.1
react-server-dom-parcel	19.0, 19.1.0, 19.1.1, 19.2.0	19.0.1, 19.1.2, 19.2.1
react-server-dom-turbopack	19.0, 19.1.0, 19.1.1, 19.2.0	19.0.1, 19.1.2, 19.2.1

  Guía actualización React:

  - https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

  A continuación, se presentan las versiones vulnerables de next.js y su respectiva actualización para corregir la vulnerabilidad.

Next.js vulnerable	Versión corregida
Versiones 15.0.0 hasta 15.5.6	15.0.5, 15.1.9, 15.2.6, 15.3.6, 15.4.8, 15.5.7
Versiones 16.0.0 hasta 16.0.6	16.0.7
Canary 14 después de 14.3.0-canary.76	Migrar a 14.x estable (14.3.x estable o superior) o actualizar a una rama parcheada (Next 15.x o 16.0.7)

  Guía actualización Next.js:

  - https://vercel.com/kb/bulletin/react2shell?utm_source

- Si la arquitectura lo permite, desactivar o reemplazar características de renderizado del servidor (SSR/RSC) temporalmente (por ejemplo, volver a un enfoque de Pages Router en Next.js) reduce temporalmente la superficie de ataque mientras se parchea.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Fortalecer la validación de entradas en el backend que recibe datos desde las aplicaciones web, específicamente en los endpoints que procesan payloads serializados. Un análisis cuidadoso de validación/normalización de inputs previene manipulaciones maliciosas. Aunque React2Shell es fundamentalmente un problema en la lógica interna, reforzar validación reduce el impacto de cargas inesperadas.

- Evaluar que entornos públicos y servicios serverless no expongan funciones innecesarias, y aplicar políticas de acceso restrictivas, roles y segmentación de red que limiten la exposición directa a Internet de aplicaciones con RSC.

Fuentes:

- https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components?utm_source
- https://nextjs.org/blog/CVE-2025-66478?utm_source
- https://github.com/kOaDT/poc-cve-2025-55182?utm_source
- https://thehackernews.com/2025/12/critical-react2shell-flaw-added-to-cisa.html
- https://nvd.nist.gov/vuln/detail/CVE-2025-55182?utm_source

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 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570