React/Next.js 远程代码执行漏洞（CVE-2025-55182/CVE-2025-66478）通告

■ 通告编号 **NS-2025-0053**	■ 发布日期 **2025-12-04**
■ 漏洞危害	**攻击者利用上述漏洞，可实现远程代码执行。**
■ TAG	React、Next.js、远程代码执行、CVE-2025-55182、CVE-2025-66478

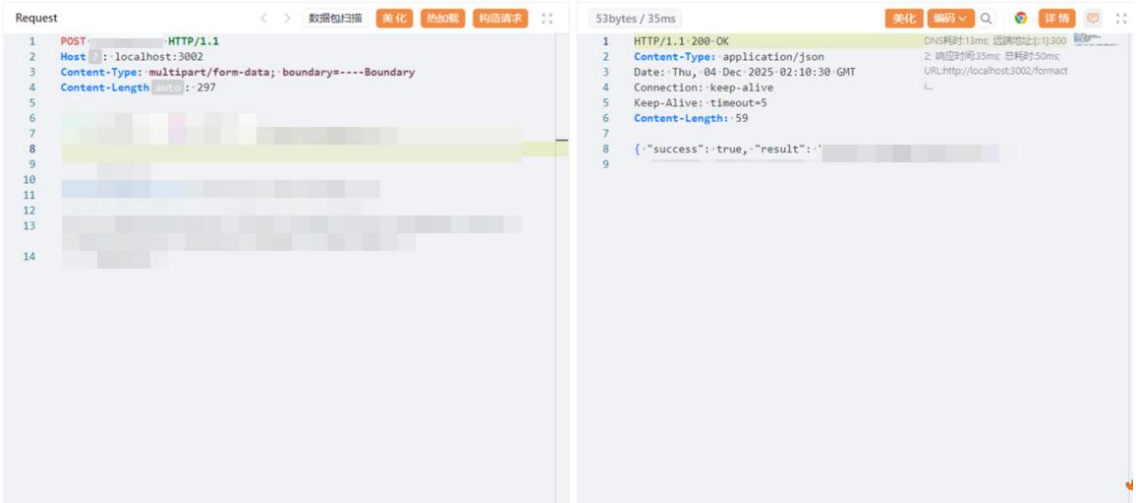
一. 漏洞概述

近日，绿盟科技 CERT 监测到 React 与 Next.js 发布安全公告，修复了 React/Next.js 远程代码执行漏洞（CVE-2025-55182/CVE-2025-66478）；由于 React Server Components 在处理 HTTP 请求时存在不安全地反序列化，未经身份验证的攻击者可通过构造特制表单调用 Node.js 内置模块，从而在目标服务器上执行任意代码，由于 Next.js 使用的 App Router 内嵌了 React 的 DOM 包，因此也受该漏洞影响。CVSS 评分 10.0，目前漏洞细节与 PoC 已公开，请相关用户尽快采取措施进行防护。

React 是 Facebook 推出的开源 JavaScript 库，采用声明式编程范式，让开发者能够高效地创建可交互的 Web 应用界面。

Next.js 是 Node.js 生态中基于 React 的开源 Web 框架，其通过 Server Actions 功能提供了后端开发能力。

绿盟科技已成功复现此漏洞：



参考链接：

https://nextjs.org/blog/CVE-2025-66478

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

二. 影响范围

受影响版本

- React Server = 19.0.0
- React Server = 19.1.0
- React Server = 19.1.1
- React Server = 19.2.0

注：包括 react-server-dom-webpack/react-server-dom-parcel/react-server-dom-turbopack

- 15.0.0 <= Next.js <= 15.0.4
- 15.1.0 <= Next.js <= 15.1.8
- 15.2.0 <= Next.js <= 15.5.6
- 16.0.0 <= Next.js <= 16.0.6
- Next.js >= 14.3.0-canary.77

注：react-router, waku, @parcel/rsc, @vitejs/plugin-rsc、rwsdk 和 RedwoodJS (RSC 模式) 等依赖 React 的框架/工具也可能受影响。

不受影响版本

- React Server = 19.0.1
- React Server = 19.1.2
- React Server = 19.2.1
- Next.js = 13.x
- Next.js = 14.x
- Next.js >= 15.0.5
- Next.js >= 15.1.9
- Next.js >= 15.2.6
- Next.js >= 15.3.6
- Next.js >= 15.4.8
- Next.js >= 15.5.7
- Next.js >= 16.0.7

注：仅使用 Client Components (Pages Router) 和 Edge Runtime 的 Next.js 应用不受影响。

三. 漏洞排查

相关用户可通过排查项目是否使用了 React Server Component(RSC)：

1、判断应用是否使用 next，react-router，waku，@parcel/rsc，@vitejs/plugin-rsc 和 rwsdk

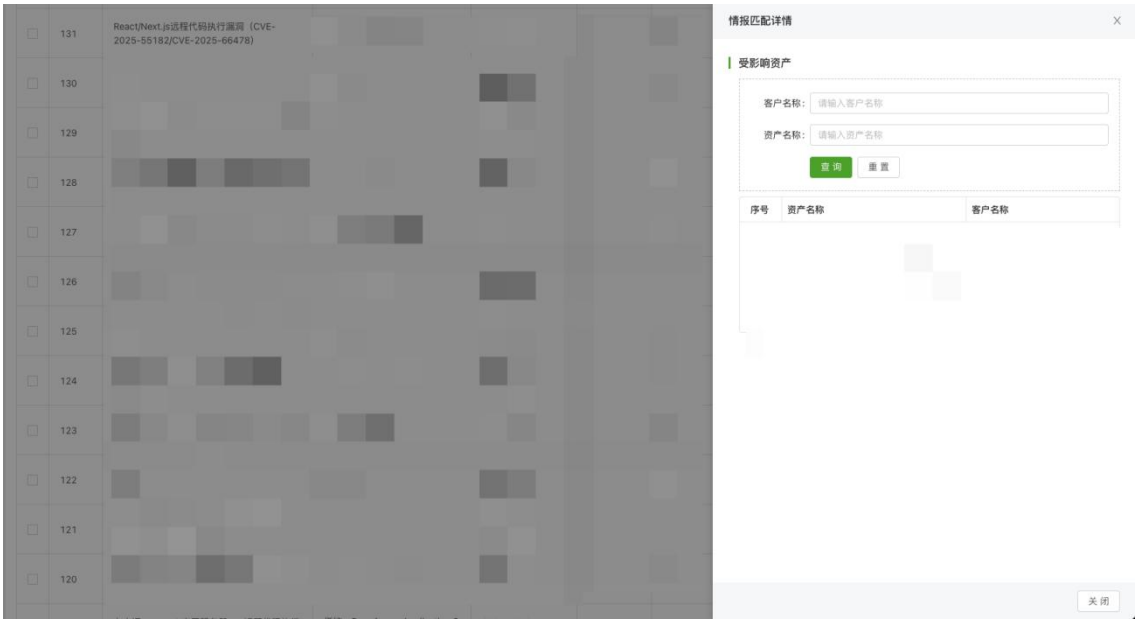
2、检查代码中是否使用了 use server/use client

若确定使用了 React Server Component(RSC)，进一步查看版本是否在受影响范围。

四. 暴露面风险排查

4.1 云端检测

绿盟科技外部攻击面管理服务（EASM）支持 CVE-2025-55182/CVE-2025-66478 漏洞风险的互联网资产排查，目前已帮助服务客户群体完成了暴露面排查，在威胁发生前及时进行漏洞预警与闭环处置。



感兴趣的客户可通过联系绿盟当地区域同事或发送邮件至 rs@nsfocus.com 安排详细的咨询交流。

4.2 工具排查

绿盟科技自动化渗透测试工具（EZ）已支持 Next.js 的服务识别和 CVE-2025-55182 漏洞风险检测，可直接使用 web 模块进行扫描。（注：企业版请联系绿盟销售人员获取）

```
[INF] 2025-12-04 11:01:48 [checkip.go:352] ip database load total:531080 records, spend :8.2 ms
[INF] 2025-12-04 11:01:48 [es.go:202] can't found es config,will not use es
[INF] 2025-12-04 11:01:48 [util.go:62] load subdomain api subdomain_api_anubis.yaml success
[INF] 2025-12-04 11:01:48 [util.go:62] load subdomain api subdomain_api_crt.yaml success
[INF] 2025-12-04 11:01:48 [util.go:62] load subdomain api subdomain_api_ip138.yaml success
[INF] 2025-12-04 11:01:48 [util.go:62] load subdomain api subdomain_api_rapid7.yaml success
[INF] 2025-12-04 11:01:48 [util.go:62] load subdomain api subdomain_api_riddler.yaml success
[INF] 2025-12-04 11:01:48 [util.go:62] load subdomain api subdomain_api_sublist3r.yaml success
[INF] 2025-12-04 11:01:48 [util.go:66] load subdomain api yaml rule: 6
[INF] 2025-12-04 11:01:58 [utils.go:547] use_poc/total_poc: 1/4844
[INF] 2025-12-04 11:01:58 [utils.go:566] type:Perfolder level:critical  name:poc-yaml-react-rsc-rce-cve-2025-55182
[INF] 2025-12-04 11:01:58 [runner.go:167] starting mitm server listen on: 127.0.0.1:2222
[*] done_http:0, undo_http:0, undo_port:0, undo_task:0, req:1/1, finger:0, vuln:0
[Vuln: poc-yaml-react-rsc-rce-cve-2025-55182]
Level: 严重
Url: http://localhost:3002/

[*] done_http:1, undo_http:0, undo_port:0, undo_task:0, req:1/2, finger:0, vuln:1
```

工具下载链接：https://github.com/m-sec-org/EZ/releases

新用户请注册 M-SEC 社区（https://msec.nsfocus.com）申请证书进行使用：

注：社区版本将于近日发布上述功能

五. 漏洞防护

5.1 官方升级

目前官方已发布新版本修复了上述漏洞，请受影响的用户尽快升级版本进行防护，下载链接：https://github.com/facebook/react/releases

https://github.com/vercel/next.js/tags

5.2 临时防护措施

若相关用户暂时无法进行升级操作，可通过下列措施进行临时缓解：

1、在不影响业务的前提下，修改配置禁用 React Server Components 功能；

2、对 Server Function 端点进行访问限制。

声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。

绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。