网络安全预警通报

2025 年第 8 期（总第 58 期）

西安交通大学网络信息中心 2025 年 12 月 05 日

【预警类型】高危预警

【预警内容】

React/Next.js 服务器组件远程代码执行漏洞（CVE-2025-55182 / CVE-2025-66478）高危利用风险通报

一、漏洞概述

安全研究团队于近期披露 React Server Components 与 Next.js App Router 中存在严重远程代码执行漏洞，编号分别为 CVE-2025-55182（React）与 CVE-2025-66478（Next.js）。该漏洞源于 react-server-dom-webpack 在处理客户端表单请求时缺乏必要的安全校验，导致攻击者可通过构造恶意表单数据，使服务器端的 Server Actions 在未授权条件下被劫持执行。

攻击者可调用 Node.js 内置模块（例如：child_process、fs），在服务器上直接执行任意系统命令、读写任意文件，最终可完全接管

服务器。该漏洞利用极为简单，仅需一次伪造的 HTTP POST 请求即可触发。

该漏洞已出现多份可复现 PoC，并有多家安全团队验证可在真实业务中稳定 RCE，风险极为突出。

二、漏洞详情

1.技术原理

漏洞类型：远程代码执行（RCE）

产生原因：

react-server-dom-webpack 在解析 Server Actions 的表单数据时，会反序列化攻击者可控的字段，并错误地允许客户端指定执行的服务端函数引用。攻击者可通过构造恶意字段，将服务端绑定对象替换为 Node.js 内置模块函数，从而执行任意代码。

攻击者能成功调用：

global.process.mainModule.require("child_process").execSync("id")

global.process.mainModule.require("child_process").execSync("whoami")

并获取系统用户身份，证明可直接执行系统命令。

2.利用条件

必要条件：目标环境使用 React Server Components 或 Next.js App Router（15.x / 16.x），后端已启用 Server Actions 功能，并且对外暴露了可被访问的表单提交接口（如 POST /formaction）。

关联风险：远程执行任意系统命令、读取或写入服务器任意文件、发起反弹 shell 及横向移动，最终取得服务器的完全控制权；该漏洞的利用无需认证，仅依靠一次恶意 POST 请求即可触发，整体风险极高。

三、漏洞影响范围

1.受影响版本

React Server Components：

React Server 19.0.0

React Server 19.0.1（部分补丁不完整）

React Server 19.1.*

React Server 19.2.0

Next.js（App Router 相关版本）：

Next.js v15.0.0 – v15.0.4

Next.js v15.1.0 – v15.1.8

Next.js v15.2.x – v15.5.6

Next.js v16.0.0 – v16.0.6

Next.js v14.3.0-canary.77 及以上 Canary 版本

2.受影响平台

Node.js 服务端（包含 Docker/K8s 部署场景）

3.威胁严重性

CVSS v3.1 评估：9.8（Critical）；CVSS v4.0 评估：9.3（Critical）

特别提醒：目前已有多份 PoC 流出，漏洞利用非常直接，威胁覆盖大量企业 Web 服务、SaaS 服务、门户系统、API 服务等。由于可直接 RCE，风险等级需按最高级别处置。

四、处置建议

1. 立即升级至官方补丁版本

React 官方已发布紧急更新，必须立即升级至以下版本：

React Server 19.0.1

React Server 19.1.2

React Server 19.2.1

Next.js 用户请同步更新至最新稳定版本，确保内置 react-server-dom-webpack 已被替换为修复版本。