Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

React2Shell Flaw in React Server Components Under Active Attack

Date of Publication

December 9, 2025

Admiralty Code

A1

TA Number

TA2025372

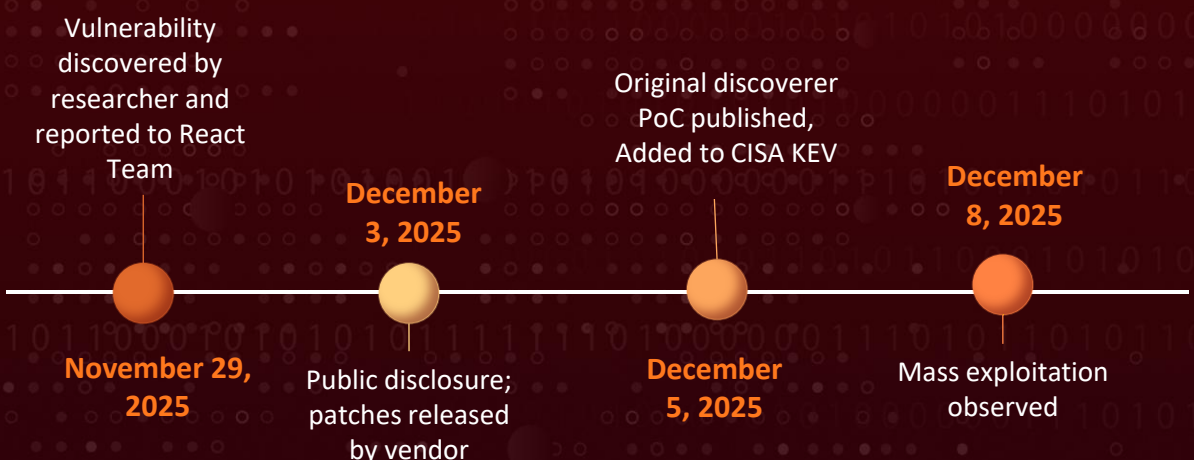
Summary

First Seen: November 29, 2025
Affected Product: Meta React Server Components
Threat Actors: Earth Lamia, Jackpot Panda and UNC5174 (aka Uteus, CL-STA-1015)
Impact: CVE-2025-55182 (React2Shell) is a CVSS 10.0 unauthenticated RCE flaw in React Server Components caused by unsafe deserialization in the Flight protocol, affecting React 19.x and frameworks like Next.js 15.x/16.x. It allows crafted POST requests to trigger arbitrary server-side JavaScript execution, leading to widespread, near-reliable compromise of internet-exposed applications. Rapid exploitation began within days of disclosure, with threat actors, including Earth Lamia, Jackpot Panda, and UNC5174, deploying cryptominers, webshells, and backdoors. Immediate patching to fixed React and Next.js versions, along with WAF protections and aggressive monitoring, is critical to mitigate ongoing mass scanning and attacks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55182	React2Shell (Meta React Server Components Remote Code Execution Vulnerability)	Meta React Server Components	✗	✓	✓

Exploitation Timeline



Vulnerability Details

#1

CVE-2025-55182, also called React2Shell, is a critical unauthenticated remote code execution (RCE) vulnerability in React Server Components (RSC), rated CVSS 10.0. The issue stems from unsafe deserialization within the RSC Flight protocol, where server-function HTTP payloads are accepted and processed without proper validation. This flaw affects React versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 and packages such as react-server-dom-webpack, react-server-dom-parcel, and react-server-dom-turbopack. Frameworks that bundle these packages, including Next.js 15.x and 16.x using the App Router, are vulnerable by default, making the exposure extremely widespread across modern web applications.

#2

The vulnerability enables attackers to send crafted POST requests to exposed RSC endpoints, triggering arbitrary JavaScript execution on the server with near-perfect reliability and no authentication. Following public disclosure on December 3, 2025, exploitation began within days, with mass scanning and opportunistic attacks observed across the internet. Because many organizations do not realize their applications rely on RSC internally, millions of sites became vulnerable automatically through framework defaults.

#3

Real-world exploitation has escalated rapidly. Attackers commonly perform reconnaissance using commands like uname, id, and whoami, often base64-encoded, before deploying cryptominers, webshells, Cobalt Strike beacons, and backdoors. Multiple threat actors, including China-nexus groups such as Earth Lamia, Jackpot Panda and UNC5174, have weaponized the flaw.

#4

Mitigation requires immediate patching, React should be updated to 19.0.1, 19.1.2, or 19.2.1, and Next.js to versions like 15.5.7 or 16.0.7, which contain the official fixes. Organizations unable to patch instantly should deploy WAF rules, network signatures, and endpoint monitoring to block malicious payloads. Given the active exploitation and large attack surface, security teams should prioritize asset inventories, continuous scanning, and log analysis to prevent or disrupt ongoing compromise attempts.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-55182	react-server-dom-webpack, react-server-dom-parcel, react-server-dom-turbopack versions: 19.0.0, 19.1.0, 19.1.1, 19.2.0 Next.js versions: 14.3.0-canary.77+, 15.x, 16.x (before 16.0.7) React Router, Waku, RedwoodSDK, @parcel/rsc, @vitejs/plugin-rsc	cpe:2.3:a:facebook:react:*:*:*:*:*:*:*:* cpe:2.3:a:vercel:next.js:*:*:*:*:*:*:node.js:*:* cpe:2.3:a:remix:react_router:*:*:*	CWE-502

Recommendations

Apply Patched React and Next.js Versions Immediately: Ensure all applications using React Server Components are upgraded to the fixed versions released in early December 2025. Update React to 19.0.1, 19.1.2, or 19.2.1, and update Next.js to 15.5.7, 16.0.7, or later. After updating, perform a full rebuild and redeployment of your application workloads. Validate the updated package versions in package.json, lockfiles, and CI/CD build artifacts to confirm that no vulnerable versions remain in use.

Inventory and Audit RSC Usage: Identify all applications using React Server Components across your environment. This includes not just Next.js but also React Router, Waku, RedwoodSDK, and any custom implementations using react-server-dom-* packages. Prioritize internet-facing applications for immediate patching.

Enable WAF Protections: If using Cloudflare, AWS WAF, or Vercel, enable RSC protection rules immediately. AWS WAF AWSManagedRulesKnownBadInputsRuleSet (version 1.24+) includes updated rules for CVE-2025-55182. These provide defense-in-depth but are not substitutes for patching.

Enable Runtime Monitoring for Node.js Process Abuse: Configure your EDR or cloud workload protection tools to alert on unusual child processes spawned by Node.js runtimes, including shells, package managers, or network utilities. React2Shell exploitation frequently results in runtime execution of commands such as uname, whoami, curl, and base64-decoded scripts. Monitoring for these behaviors provides early detection of ongoing or successful exploitation attempts.

Potential MITRE ATT&CK TTPs

TA0010 Exfiltration	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0040 Impact	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0007 Discovery	T1505.003 Web Shell	T1505 Server Software Component
T1068 Exploitation for Privilege Escalation	T1588.005 Exploits	T1588.006 Vulnerabilities	T1588 Obtain Capabilities
T1190 Exploit Public-Facing Application	T1059.007 JavaScript	T1059.004 Unix Shell	T1059 Command and Scripting Interpreter
T1082 System Information Discovery	T1057 Process Discovery	T1083 File and Directory Discovery	T1105 Ingress Tool Transfer
T1041 Exfiltration Over C2 Channel	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1496 Resource Hijacking
T1567 Exfiltration Over Web Service	T1036 Masquerading		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	206[.]237.3.150, 45[.]77.33.136, 143[.]198.92.82, 183[.]6.80.214, 115[.]42[.]60[.]223, 140[.]99[.]223[.]178, 156[.]234[.]209[.]103, 38[.]162[.]112[.]141, 45[.]32[.]158[.]54, 46[.]36[.]37[.]85, 47[.]84[.]79[.]46, 95[.]169[.]180[.]135, 45.134.174[.]235
URLs	hxxp://46[.]36[.]37[.]85:12000/sex[.]sh, hxxp://115[.]42[.]60[.]223:61236/slt, hxxp://45[.]32[.]158[.]54/5e51aff54626ef7f/x86_64, hxxp://115[.]42[.]60[.]223:61236/slt, hxxp://156[.]234[.]209[.]103:20912/get[.]sh, hxxp://156[.]234[.]209[.]103:20913/get[.]sh, hxxp://45[.]32[.]158[.]54/5e51aff54626ef7f/x86_64, hxxp://46[.]36[.]37[.]85:12000/sex[.]sh, hxxp://95[.]169[.]180[.]135:8443/pamssod, hxxp://res[.]qiqigece[.]top/nginx1, hxxp://146.88.129[.]138:5511/443nb64, hxxps://raw[.]githubusercontent[.]com/C3Pool/xmrig_setup/master/setup_c3pool_miner[.]sh, hxxps://sup001[.]oss-cn-hongkong[.]aliyuncs[.]com/123/python1[.]sh
Domains	reactcdn[.]windowserrorapis[.]com, res[.]qiqigece[.]top
SHA256	a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4, 4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b,

TYPE	VALUE
SHA256	1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665, 18c68a982f91f665effe769f663c51cb0567ea2bfc7fab6a1a40d4fe50fc382b, 1a3e7b4ee2b2858dbac2d73dd1c52b1ea1d69c6ebb24cc434d1e15e43325b74e, 1cdd9b0434eb5b06173c7516f99a832dc4614ac10dda171c8eed3272a5e63d20, 1e31dc074a4ea7f400cb969ea80e8855b5e7486660aab415da17591bc284ac5b, 2b0dc27f035ba1417990a21dafb361e083e4ed94a75a1c49dc45690ecf463de4, 2ca913556efd6c45109fd8358edb18d22a10fb6a36c1ab7b2df7594cd5b0adbc, 4ff096fbea443778fec6f960bf2b9c84da121e6d63e189aebaaa6397d9aac948, 55ae00bc8482afd085fd128965b108cca4adb5a3a8a0ee2957d76f33edd5a864, 62e9a01307bcf85cdaeecafd6efb5be72a622c43a10f06d6d6d3b566b072228d, 7d25a97be42b357adcc6d7f56ab01111378a3190134aa788b1f04336eb924b53, 7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a, 9c931f7f7d511108263b0a75f7b9fcbbf9fd67ebcc7cd2e5dcd1266b75053624, ac2182dfbf56d58b4d63cde3ad6e7a52fed54e52959e4c82d6fc999f20f8d693, ac7027f30514d0c00d9e8b379b5ad8150c9827c827dc7ee54d906fc2585b6bf6, b38ec4c803a2d84277d9c598bfa5434fb8561ddad0ec38da6f9b8ece8104d787, bc31561c44a36e1305692d0af673bc5406f4a5bb2c3f2ffdb613c09b4e80fa9f, bf602b11d99e815e26c88a3a47eb63997d43db8b8c60db06d6fbddf386fd8c4a, d704541cde64a3eef5c4f80d0d7f96dc96bae8083804c930111024b274557b16, d9313f949af339ed9fafb12374600e66b870961eeb9b2b0d4a3172fd1aa34ed0, e2d7c8491436411474cef5d3b51116ddecfee68bab1e15081752a54772559879, ebdb85704b2e7ced3673b12c6f3687bc0177a7b1b3caef110213cc93a75da837,

TYPE	VALUE
SHA256	f88ce150345787dd1bcfbc301350033404e32273c9a140f22da80810e3a3f6ea, fc9e53675e315edeea2292069c3fbc91337c972c936ca0f535da01760814b125, 33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f,

Patch Details

Patched React Versions:
- react-server-dom-webpack: 19.0.1, 19.1.2, 19.2.1
- react-server-dom-parcel: 19.0.1, 19.1.2, 19.2.1
- react-server-dom-turbopack: 19.0.1, 19.1.2, 19.2.1

Patched Next.js Versions:
- 16.0.7, 15.5.7, 15.4.8, 15.3.6, 15.2.6, 15.1.9, 15.0.5

Note: CVE-2025-66478 was initially assigned separately for Next.js but was rejected as a duplicate since the root cause lies in the underlying React packages.

Link:
https://github.com/facebook/react/security/advisories/GHSA-fv66-9v8q-g76r

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

References

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

https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/

https://github.com/rapid7/metasploit-framework/pull/20747

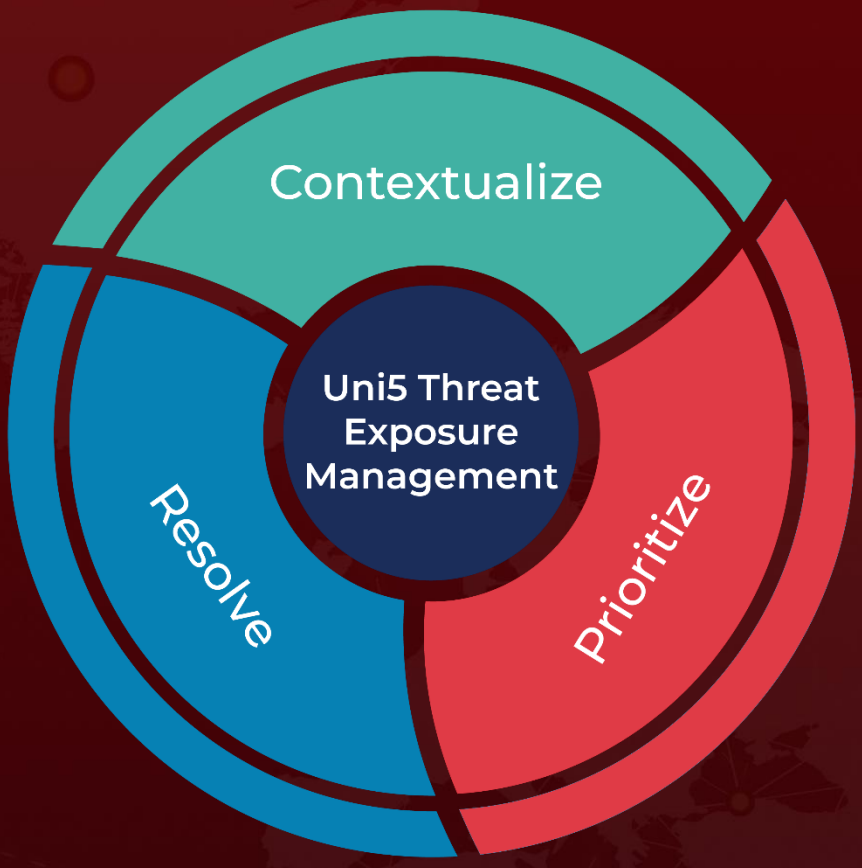
https://unit42.paloaltonetworks.com/cve-2025-55182-react-and-cve-2025-66478-next/

https://www.rapid7.com/blog/post/etr-react2shell-cve-2025-55182-critical-unauthenticated-rce-affecting-react-server-components/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 9, 2025 • 3:30 AM

More at www.hivepro.com