Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

React2Shell Flaw in React Server Components Under Active Attack

Date of Publication	Date of Publication	Admiralty Code	TA Number
December 9, 2025	December 16, 2025	A1	TA2025372

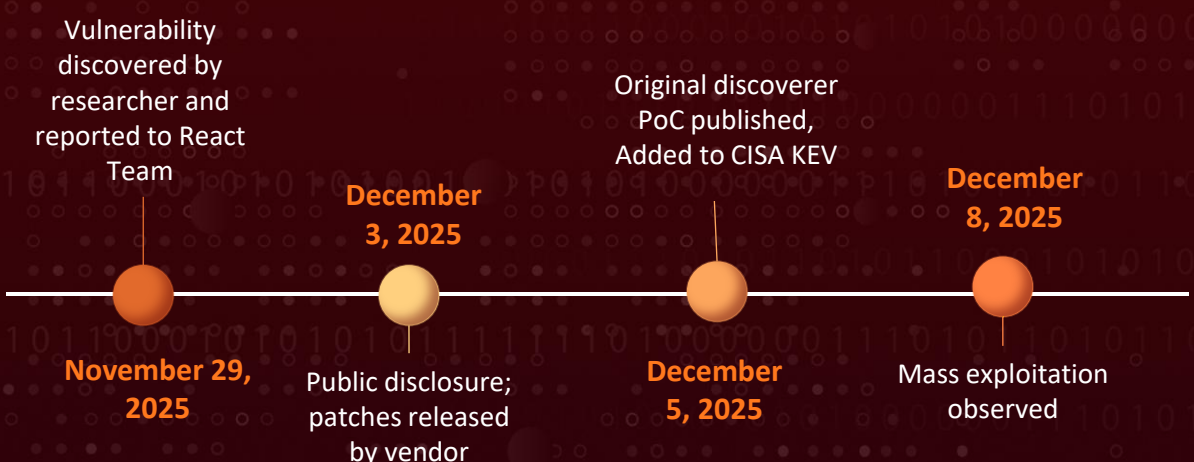
Summary

First Seen: November 29, 2025
Affected Product: Meta React Server Components
Threat Actors: Earth Lamia (aka UNC5454), Jackpot Panda and UNC5174 (aka Uteus, CL-STA-1015), UNC6600, UNC6588, UNC6603, UNC6595, UNC5342
Malware: XMRig, Sliver, PeerBlight, EtherRAT, Snowlight, Vshell, Noodle RAT (aka ANGRYREBEL.LINUX), KSwapDoor, Auto-color, Minocat, Compood, and Hisonic
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 of CVE-2025-55182 has escalated rapidly. Attackers typically begin with base64-encoded reconnaissance commands such as uname, id, and whoami, followed by deployment of post-exploitation payloads. Observed malware includes XMRig cryptominers, Sliver implants, PeerBlight, ANGRYREBEL.LINUX, KSwapDoor, and Auto-color Linux backdoors, Cobalt Strike beacons, SNOWLIGHT/VSHELL loaders, EtherRAT implants, MINOCAT tunnelers, and custom backdoors (COMPOOD, HISONIC). Exploitation spans financially motivated and espionage-driven activity, with China-nexus groups (e.g., Earth Lamia/UNC5454, Jackpot Panda, UNC5174, UNC6586, UNC6600, UNC6603, UNC6588, UNC6595), Iran-nexus, and DPRK-aligned (including UNC5342) actors actively leveraging the vulnerability.

#4

DPRK-linked campaigns have introduced EtherRAT, a stealthy implant downloading legitimate Node.js binaries and using Ethereum smart contracts for C2, enabling long-term access beyond traditional blocking. The diversity of malware families, loaders, RATs, and persistence mechanisms, masquerading, indicates React2Shell has matured into sustained intrusions.

#5

Mitigation requires immediate patching: React should be updated to 19.0.1, 19.1.2, or 19.2.1, and Next.js to 15.5.7 or 16.0.7, which contain the official fixes. Organizations unable to patch immediately should deploy WAF rules, network signatures, and enhanced endpoint monitoring to block malicious payloads and detect post-exploitation activity.

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	TA0006 Credential Access	TA0008 Lateral Movement
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	T1505.003 Web Shell	T1053 Scheduled Task/Job
T1552.001 Credentials In Files	T1552 Unsecured Credentials	T1102 Web Service	T1053.003 Cron
T1543.002 Systemd Service	T1543 Create or Modify System Process	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution
T1070.006 Timestomp	T1070 Indicator Removal	T1036 Masquerading	T1140 Deobfuscate/Decode Files or Information
T1090 Proxy	T1568 Dynamic Resolution	T1568.003 DNS Calculation	T1505 Server Software Component

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, 80[.]64[.]16[.]241, 47[.]236[.]194[.]231, 216[.]238[.]68[.]16, 45[.]153[.]34[.]172, 37[.]27[.]217[.]205, 212[.]237[.]120[.]249, 5[.]161[.]227[.]224, 154[.]26[.]190[.]6, 104[.]238[.]61[.]32, 193[.]34[.]213[.]150, 154[.]89[.]152[.]240, 172[.]245[.]79[.]16, 47[.]84[.]82[.]8, 8[.]222[.]213[.]56, 216[.]158[.]232[.]43, 185[.]229[.]32[.]220, 185[.]247[.]224[.]41, 49[.]51[.]230[.]175, 23[.]226[.]71[.]197, 23[.]226[.]71[.]200, 23[.]226[.]71[.]209, 82[.]163[.]22[.]139, 216[.]158[.]232[.]43
Domains	reactcdn[.]windowserrorapis[.]com, res[.]qiqigece[.]top, conclusion-ideas-cover-customise[.]trycloudflare[.]com, api[.]hellknight[.]xyz, gfxnick[.]emerald[.]usbx[.]me,

TYPE	VALUE
Domains	Api[.]qtss[.]cc, anywherehost[.]site, inerna1[.]site, ip[.]inovanet[.]pt, keep[.]camdvr[.]org, t[.]cnzzs[.]co, ax29g9q123[.]anondns[.]net, aws[.]orgserv[.]dnsnet[.]cloud[.]anondns[.]net, mail[.]wrufff[.]de, tr[.]earn[.]top, proxy1[.]ip2worlds[.]vip
URLs	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, hxxp[:]//115[.]42[.]60[.]223[:]61236/slt , hxxp[:]//115[.]42[.]60[.]223[:]61236/slt, hxxp[:]//156[.]234[.]209[.]103[:]20912/get[.]sh, hxxp[:]//156[.]234[.]209[.]103[:]20913/get[.]sh, hxxp[:]//46[.]36[.]37[.]85[:]12000/sex[.]sh, hxxp[:]//95[.]169[.]180[.]135[:]8443/pamssod, hxxp[:]//res[.]qiqigece[.]top/nginx1, hxxps[:]//raw[.]githubusercontent[.]com/C3Pool/xmrig_setup/master/setup_c3pool_miner[.]sh, hxxps[:]//sup001[.]oss-cn-hongkong[.]aliyuncs[.]com/123/python1[.]sh, hxxp[:]//193[.]34[.]213[.]150/nuts/x, hxxp[:]//193[.]34[.]213[.]150/nuts/lc, hxxp[:]//23[.]132[.]164[.]54/bot, hxxp[:]//178[.]16[.]55[.]224[:]80/sh, hxxp[:]//eleveratech[.]com[:]8080/healthcheck123[.]dll, hxxps[:]//gist[.]githubusercontent[.]com[:]443/demonic-agents/39e943f4de855e2aef12f34324cbf150/raw/e767e1cef1c35738689ba4df9c6f7f29a6afba1a/setup_c3pool_miner[.]sh, hxxp[:]//eleveratech[.]com[:]8080/healthcheck[.]dll, hxxp[:]//2[.]56[.]176[.]35[:]443/healthcheck[.]dll, hxxps[:]//raw[.]githubusercontent[.]com[:]443/c3pool/xmrig_setup/master/setup_c3pool_miner[.]bat, hxxp[:]//95[.]169[.]180[.]135, hxxps[:]//api[.]hellknight[.]xyz/js, hxxp[:]//59[.]7[.]217[.]245[:]7070/c[.]sh,

TYPE	VALUE
URLs	hxxp[:]//help[.]093214[.]xyz[:]9731/fn32[.]sh, hxxp[:]//192[.]210[.]160[.]141[:]80/, hxxp[:]//114[.]46[.]135[.]44[:]80/, hxxp[:]//38[.]162[.]112[.]141, hxxp[:]//res[.]qiqigece[.]top/, hxxps[:]//ivk[.]sh/nxt2, hxxp[:]//45[.]134[.]174[.]235[:]443/a2[.]sh, hxxp[:]//31[.]56[.]27[.]76/, hxxp[:]//193[.]24[.]123[.]68[:]3001/, hxxp[:]//217[.]60[.]249[.]228[:]8000/stx[.]sh, hxxp[:]//89[.]144[.]31[.]18/nuts/x86, hxxp[:]//171[.]252[.]32[.]135[:]7700, hxxp[:]//78[.]153[.]140[.]16/curl-amd64, hxxp[:]//38[.]165[.]44[.]205/api, hxxp[:]//78[.]153[.]140[.]16/curl-aarch64, hxxp[:]//80[.]64[.]16[.]241/re[.]sh, hxxp[:]//38[.]165[.]44[.]205/s, hxxp[:]//47[.]236[.]194[.]231[:]9001/setup2[.]sh, hxxp[:]//anywherehost[.]site/xms/k1[.]sh?grep, hxxp[:]//anywherehost[.]site/xms/kill2[.]sh, hxxp[:]//anywherehost[.]site/xms/su, hxxp[:]//anywherehost[.]site/xms/t1[.]ps1, hxxp[:]//anywherehost[.]site/xb/runner[.]zip, hxxp[:]//anywherehost[.]site/xb/systemd-devd[.]$(uname -m), hxxp[:]//inerna1[.]site/xms/k1[.]sh, hxxp[:]//ip[.]inovanet[.]pt/systemprofile[.]zip, hxxp[:]//inerna1[.]site/xb/systemd-devd[.]x86_64, hxxp[:]//inerna1[.]site/xb/runner[.]zip, hxxp[:]//inerna1[.]site/xms/t1[.]ps1, hxxp[:]//superminecraft[.]net[.]br[:]3000/sex[.]sh, hxxp[:]//216[.]158[.]232[.]43[:]12000/sex[.]sh, hxxp[:]//keep[.]camdvr[.]org[:]8000/BREAKABLE_PARABLE5, hxxp[:]//185[.]229[.]32[.]220[:]21642/2lt4de8wgl54wtjgo8/winds, hxxp[:]//keep[.]camdvr[.]org[:]8000/d5[.]sh, hxxp[:]//keep[.]camdvr[.]org[:]8000/BREAKABLE_PARABLE10, hxxp[:]//47[.]84[.]82[.]8/index, hxxp[:]//47[.]84[.]82[.]8/upload, hxxp[:]//8[.]222[.]213[.]56/index, hxxp[:]//104[.]238[.]61[.]32[:]8080/zold, hxxp[:]//ax29g9q123[.]anondns[.]net, hxxps[:]//tr[.]earn[.]top/Log[.]php?id=, hxxp[:]//146[.]88[.]129[.]138[:]5511/443nb64, hxxp[:]//193[.]34[.]213[.]150/nuts/x86, hxxp[:]//139[.]59[.]59[.]33[:]9004/setup2[.]sh, hxxp[:]//128[.]199[.]194[.]97[:]9003/setup2[.]sh, hxxp[:]//154[.]89[.]152[.]240/check[.]sh,

TYPE	VALUE
URLs	hxxp[:]//78[.]153[.]140[.]16/kinsing, hxxp[:]//78[.]153[.]140[.]16/kinsing_aarch64, hxxp[:]//78[.]153[.]140[.]16/libsystem[.]so, hxxp[:]//38[.]165[.]44[.]205/1, hxxp[:]//193[.]34[.]213[.]150/nuts/bolts, hxxp[:]//45[.]32[.]158[.]54/5e51aff54626ef7f/x86_64, hxxp[:]//45[.]76[.]155[.]14/vim, hxxp[:]//103[.]135[.]101[.]15/wocaosinm[.]sh, hxxp[:]//31[.]56[.]27[.]97/scripts/4thepool_miner[.]sh, hxxp[:]//39[.]97[.]229[.]220[:]8006/httd, hxxp[:]//38[.]165[.]44[.]205/k, hxxp[:]//vps-zap812595-1[.]zap-srv[.]com[:]3000/sex[.]sh, hxxp[:]//help[.]093214[.]xyz[:]9731/FF22, hxxps[:]//api[.]qtss[.]cc[:]443/en/about?source=redhat&id=v1[.]0, hxxps[:]//api[.]qtss[.]cc[:]443/en/about?source=redhat&id=v1[.]1, hxxps[:]//api[.]qtss[.]cc[:]443/en/about?source=redhat&id=v1[.]2
File path	/lib/systemd/system/systemd-agent[.]service, /bin/systemd-daemon, /etc/init/systemd-agent[.]conf, /usr/bin/sshd-agent, ~/[.]config/[.]system-monitor/[.]sys-mon, /tmp/[.]system-update/, /home/<user>/[.]systemd-utils/conf
SHA1	be9473e2a27d1828441ef78356e75908cf27eb68, 95592fc55945b243ae518fb3379440517654b351, b66e7b8f153779ae8521248b502fcf5e5116b3af, 6bd5c6af884d46638ebc60434cfd35b37c1d3dd4, 3c92104b70ed063dc34419612742e08fc67a225d, 1539b2eb380fdf7c5ddc7c017118a81cf82bf774, e3dd33183ce13cbd184a7ebbe70edab97bb0f5cc, 8907872767c587733bdaa7d91dab2f9cb75d21e1, 5619b1c26a23919a2ea1e698ece953455da2fa95, 356754e7a570deb05dcd5b6f27b70cf5cb2d009f, dc057522e04f37a6143cf6ce9b5d4a19aab8ef7a, 86d70f7ca27844ad22fc733cfbddc6d1fb4ccc2d, 59de54c4cb7ccc1602c90d8afe2efc071751d9ae, fdc0b9324aac30632432914277a28eee402557b5, 446bb6ba79c699c1f76cfa1624805af863502bee, d04be880dd2dd2e8813edeb1fde4a73d680850d8, 259cb26c420dbf799ff52690e78e713f31f927f9,

TYPE	VALUE
SHA1	c270d7ea30c43f37226d34d26ea4e3289a485a60, fc32155be390245e28815310f23558615894f59f, 888c22017f8df53b04cc9f1bae4562e448b2881f, 38c56b5e1489092b80c9908f04379e5a16876f01, 3ca62bccec20e358592c18fd2cd23e0818dfc6b0, 264e1a820b8b3bbd13325955f06aff2678c69935, 20e1465fd07f0d4e19c299fb0d9af8e5ec1b21d2, 6e43e26fa62dfa89fe8b016dc831a9ec44507af9, d6e97c9783f0907f1ee9415736816e272a9df060, 732226c0966fe29116b147e893c35ce7df1c8f1a, be86823d73a01266b096dab1628cfa2e4ca77265, 7fe3826fc7b90e20c9fe76a7891eff350d73b6b3, 7c8010d9ab6dfdc7a99aba7075a793260acbf2b8, 91152e6ffe0474b06bb52f41ab3f3545ac360e64, 5d368356bd49c4b8e3c423c10ba777ff52a4f32a, 34551bca762be99d732c0ced6ad8b0a2f7b11ad7, 470ce679589e1c3518c3ed2b818516f27ccad089, c67e8aa881317cb32d7c36b2e3c0c5cfa21bf5e3, 2937c58115c131ae84a1b2a7226c666f6a27ef88, 122334aefafbc5a82782ee1de1029b95b88ff278, fa5ff1c91a108917db6d593238c84d2e78ad16de, ec24725661a1c3bf2fae0109b9e83f0342d23a79, 1b5aba88ba7c4011d081b499ce6009df69e5dbcf, 1ce4b6a89d2daa0cab820711d8424a7676ef5ff2, 0972859984decfaf9487f9a2c2c7f5d2b03560a0
SHA256	a605a70d031577c83c093803d11ec7c1e29d2ad530f8e95d9a729c3818c7050d, 776850a1e6d6915e9bf35aa83554616129acd94e3a3f6673bd6ddaec530f4273, 0f0f9c339fcc267ec3d560c7168c56f607232cbeb158cb02a0818720a54e72ce, 3854862bb3ee623f95d91fa15b504e2bbc30e23f1a15ad7b18aedb127998c79c, 2cd41569e8698403340412936b653200005c59f2ff3d39d203f433adb2687e7f, 65d840b059e01f273d0a169562b3b368051cfb003e301cc2e4f6a7d1907c224a

TYPE	VALUE
SHA256	a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4, 4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b, 1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665, 18c68a982f91f665effe769f663c51cb0567ea2bfc7fab6a1a40d4fe50fc382b, 1a3e7b4ee2b2858dbac2d73dd1c52b1ea1d69c6ebb24cc434d1e15e43325b74e, 1cdd9b0434eb5b06173c7516f99a832dc4614ac10dda171c8eed3272a5e63d20, 1e31dc074a4ea7f400cb969ea80e8855b5e7486660aab415da17591bc284ac5b, 2b0dc27f035ba1417990a21dafb361e083e4ed94a75a1c49dc45690ecf463de4, 2ca913556efd6c45109fd8358edb18d22a10fb6a36c1ab7b2df7594cd5b0adbc, 4ff096fbea443778fec6f960bf2b9c84da121e6d63e189aebaaa6397d9aac948, 55ae00bc8482afd085fd128965b108cca4adb5a3a8a0ee2957d76f33edd5a864, 62e9a01307bcf85cdaeecafd6efb5be72a622c43a10f06d6d6d3b566b072228d, 7d25a97be42b357adcc6d7f56ab01111378a3190134aa788b1f04336eb924b53, 7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a, 9c931f7f7d511108263b0a75f7b9fcbbf9fd67ebcc7cd2e5dcd1266b75053624, ac2182dfbf56d58b4d63cde3ad6e7a52fed54e52959e4c82d6fc999f20f8d693, ac7027f30514d0c00d9e8b379b5ad8150c9827c827dc7ee54d906fc2585b6bf6, b38ec4c803a2d84277d9c598bfa5434fb8561ddad0ec38da6f9b8ece8104d787, bc31561c44a36e1305692d0af673bc5406f4a5bb2c3f2ffdb613c09b4e80fa9f, bf602b11d99e815e26c88a3a47eb63997d43db8b8c60db06d6fbddf386fd8c4a, d704541cde64a3eef5c4f80d0d7f96dc96bae8083804c930111024b274557b16, d9313f949af339ed9fafb12374600e66b870961eeb9b2b0d4a3172fd1aa34ed0,

TYPE	VALUE
SHA256	e2d7c8491436411474cef5d3b51116ddecfee68bab1e15081752a54772559879, ebdb85704b2e7ced3673b12c6f3687bc0177a7b1b3caef110213cc93a75da837, f88ce150345787dd1bcfbc301350033404e32273c9a140f22da80810e3a3f6ea, fc9e53675e315edeea2292069c3fbc91337c972c936ca0f535da01760814b125, 33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f, df3f20a961d29eed46636783b71589c183675510737c984a11f78932b177b540, 92064e210b23cf5b94585d3722bf53373d54fb4114dca25c34e010d0c010edf3, 0bc65a55a84d1b2e2a320d2b011186a14f9074d6d28ff9120cb24fcc03c3f696, 13675cca4674a8f9a8fabe4f9df4ae0ae9ef11986dd1dcc6a896912c7d527274, 1f3f0695c7ec63723b2b8e9d50b1838df304821fcb22c7902db1f8248a812035, 33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f, a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4, 1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665, 18c68a982f91f665effe769f663c51cb0567ea2bfc7fab6a1a40d4fe50fc382b, 1a3e7b4ee2b2858dbac2d73dd1c52b1ea1d69c6ebb24cc434d1e15e43325b74e, 1cdd9b0434eb5b06173c7516f99a832dc4614ac10dda171c8eed3272a5e63d20, 1e31dc074a4ea7f400cb969ea80e8855b5e7486660aab415da17591bc284ac5b, 2b0dc27f035ba1417990a21dafb361e083e4ed94a75a1c49dc45690ecf463de4, 2ca913556efd6c45109fd8358edb18d22a10fb6a36c1ab7b2df7594cd5b0adbc, 4ff096fbea443778fec6f960bf2b9c84da121e6d63e189aebaaa6397d9aac948, 55ae00bc8482afd085fd128965b108cca4adb5a3a8a0ee2957d76f33edd5a864, 62e9a01307bcf85cdaeecafd6efb5be72a622c43a10f06d6d6d3b566b072228d, 7d25a97be42b357adcc6d7f56ab01111378a3190134aa788b1f04336eb924b53,

TYPE	VALUE
SHA256	7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a, 9c931f7f7d511108263b0a75f7b9fcbbf9fd67ebcc7cd2e5dcd1266b75053624, ac2182dfbf56d58b4d63cde3ad6e7a52fed54e52959e4c82d6fc999f20f8d693, ac7027f30514d0c00d9e8b379b5ad8150c9827c827dc7ee54d906fc2585b6bf6, b38ec4c803a2d84277d9c598bfa5434fb8561ddad0ec38da6f9b8ece8104d787, bc31561c44a36e1305692d0af673bc5406f4a5bb2c3f2ffdb613c09b4e80fa9f, bf602b11d99e815e26c88a3a47eb63997d43db8b8c60db06d6fbddf386fd8c4a, d704541cde64a3eef5c4f80d0d7f96dc96bae8083804c930111024b274557b16, d9313f949af339ed9fafb12374600e66b870961eeb9b2b0d4a3172fd1aa34ed0, e2d7c8491436411474cef5d3b51116ddecfee68bab1e15081752a54772559879, 4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b
Monero Wallet	44VvVLU2Vmja6gTMbhNHAzc7heYTiT7V mQEXkjdaYo6K41WqH8qWw1CL8wKAAgz5 xLYT3XL3pb9KCUZS7PPZbzUGCCpZ9Ee, 42NTfUjbU3Gj536zubU7vpjfC7X9DPEC ciwbCXrrjBk5KqkJS1Xq4saVgQLP1yqU YHKzn7apt1p3W6mDWm87n3nwDEmWeSh

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/

https://www.trendmicro.com/en_us/research/25/l/CVE-2025-55182-analysis-poc-itw.html

https://www.wiz.io/blog/nextjs-cve-2025-55182-react2shell-deep-dive

https://www.sysdig.com/blog/etherrat-dprk-uses-novel-ethereum-implant-in-react2shell-attacks

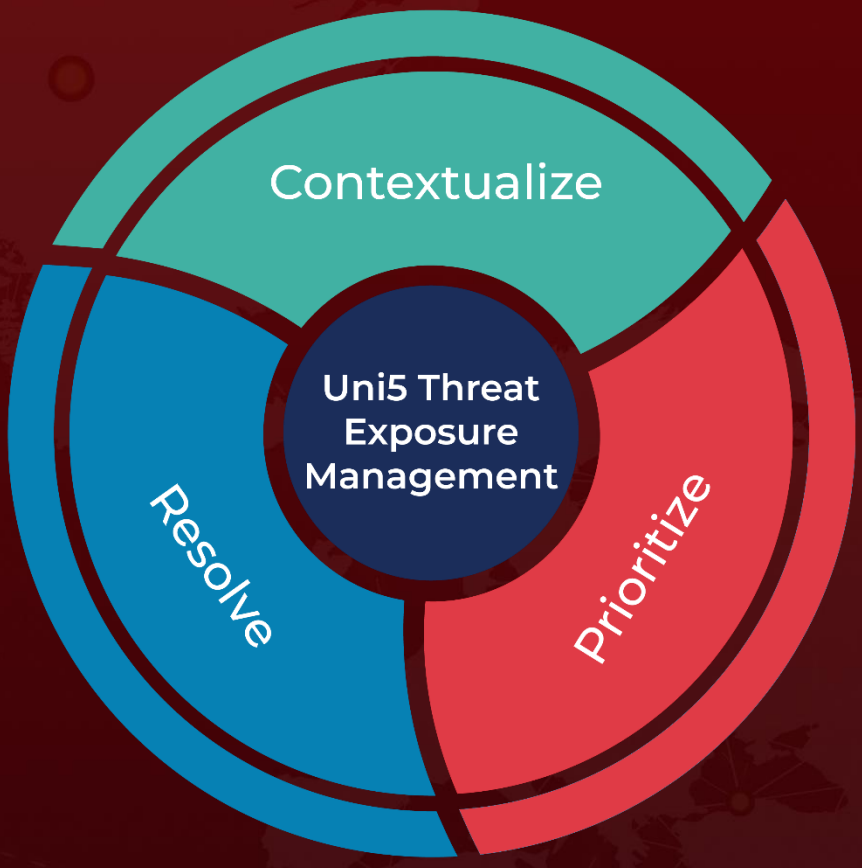
https://www.huntress.com/blog/peerblight-linux-backdoor-exploits-react2shell

https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182

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