

Multiple Threat Actors Leveraging CVE-2025-55182 (React2Shell)

By The Hivemind

Archived: 2026-07-28 02:01:00 UTC



Verticals Targeted: Technology

Regions Targeted: Unspecified

Related Families: KSwapDoor, EtherRAT, Noodle RAT, SNOWLIGHT, VShell, Cobalt Strike, XMRig, Mirai, Others

Executive Summary

Multiple vendors have observed active exploitation of CVE-2025-55182, a critical remote code execution vulnerability in React Server Components and frameworks like Next.js. Multiple threat actors, including China-nexus and North Korea-nexus APTs and criminal threat actors have been observed leveraging CVE-2025-55182.

Key Takeaways

- Multiple threat actors have been observed exploiting CVE-2025-55182, known as React2Shell.
- Post-exploitation activity includes reconnaissance via Base64-encoded commands, deployment of cryptominers such as XMRig, Cobalt Strike beacons for Linux, web shells disguised as React file managers, and RATs like EtherRAT and Noodle RAT.

- Activity clusters show involvement from suspected DPRK actors using EtherRAT in conjunction with Contagious Interview campaigns, as well as Chinese-nexus initial access brokers deploying SNOWLIGHT and VShell.
- Immediate patching to hardened versions of React (19.0.1+) and Next.js (15.x/16.x patched releases) is the primary mitigation, supplemented by layered defenses to detect post-compromise behaviors.

What is CVE-2025-55182 (React2Shell)?

Palo Alto's Unit 42 researchers have [documented](#) widespread scanning and exploitation attempts following the public disclosure of [CVE-2025-55182](#) on December 3, 2025. This flaw stems from insecure deserialization in the Flight protocol used by React Server Components, enabling unauthenticated remote code execution with near-perfect reliability against default configurations. The vulnerability affects React versions 19.0 through 19.2 and multiple Next.js releases, along with other frameworks bundling vulnerable react-server packages.

Exploitation begins with automated probes that fingerprint vulnerable endpoints, often using simple arithmetic checks executed via shell commands. Successful compromises trigger rapid reconnaissance: attackers decode and run Base64 strings to execute commands such as `uname -a`, `id`, `hostname -I`, and enumeration of `/etc/hosts` and `/etc/resolv.conf`. This gathers system details, privilege levels, network interfaces, and potential cloud environment indicators.

Payload delivery frequently leverages `wget` or `curl` to retrieve malicious scripts or architecture-specific droppers, which are immediately executed. Observed chains include conditional logic to ensure execution even if one downloader fails. Cryptomining installations target XMRig configurations, with miners configured to specific Monero wallets. In container environments, attackers have attempted Mirai variant deployments via BusyBox utilities, though many were blocked.

Advanced threats include Cobalt Strike deployments using CrossC2-generated Linux beacons, initiated through reverse shells or scripted downloads renamed to benign-sounding files. Web shells, retrieved from public repositories and modified to cycle through ports, provide interactive file management, command execution, and data exfiltration capabilities while attempting persistence via `nohup`.

Threat Actors Observed Leveraging React2Shell

UNC5174

UNC5174, also known as Uteus, is a Chinese state-sponsored threat actor suspected of ties to China's Ministry of State Security and acting as an initial access broker. They have been exploiting the critical React2Shell vulnerability to drop SNOWLIGHT, a stealthy malware dropper that fetches and executes additional payloads, often including the VShell remote access trojan for persistence, remote control, and lateral movement.

Earth Lamia

Earth Lamia, a China-nexus threat actor, specializes in exploiting web application vulnerabilities to target organizations in Latin America, the Middle East, Southeast Asia, and beyond, across multiple sectors including

finance, logistics, retail, IT, universities, and government. Within hours of CVE-2025-55182 disclosure on December 3, 2025, Amazon Web Services [observed](#) exploitation attempts from infrastructure linked to Earth Lamia. Earth Lamia's activity involved reconnaissance, file operations, and potential credential theft or backdoor deployment.

Jackpot Panda

Jackpot Panda, a China-nexus state-sponsored threat actor, primarily conducts cyber espionage targeting entities in East and Southeast Asia, often focused on online gambling operations, corruption, and domestic security intelligence. Within hours of CVE-2025-55182 disclosure on December 3, 2025, Amazon Web Services [observed](#) exploitation attempts from infrastructure linked to Jackpot Panda. Jackpot Panda's activity involved rapid integration of public PoCs, automated scanning with evasion tactics, reconnaissance commands, and multi-vulnerability campaigns.

HiddenOrbit (RedRelay)

In a [post](#) regarding CVE-2025-55182 related activity, Recorded Future analysts stated the IP address 143.198.92[.]82, observed alongside this activity, is highly likely an exit node for HiddenOrbit (aka RedRelay), a Chinese anonymization relay network used by state-sponsored threat actors. This infrastructure was observed conducting scanning and exploitation attempts against the React2Shell vulnerability shortly after its disclosure.

Other China-nexus Threat Actors

Google Threat Intelligence Group [observed](#) multiple China-nexus threat actors leveraging React2Shell, including the following:

- UNC6586: Deployed SNOWLIGHT downloader for further payloads.
- UNC6588: Downloaded COMPOOD backdoor, which masquerades as Vim.
- UNC6595: Deployed Angryrebel.Linux RAT, targeting VPS infrastructure.
- UNC6600: Deployed MINOCAT tunneler.
- UNC6603: Deployed updated HISONIC backdoor.

UNC5342

UNC5342, a North Korea linked APT was observed exploiting React2Shell. Sysdig [reported](#) UNC5342 deploying EtherRAT malware just two days after the vulnerability was disclosed.

Opportunistic and Criminal Threat Actors

Cybercriminals and botnets have been observed leveraging the vulnerability to deploy XMRig cryptominers, PeerBlight backdoor, reverse proxies, and Go-based implants. There has also been widespread automated scanning/exploitation by non-state actors using Mirai-based botnets. Given the vulnerability's deterministic nature and the extensive deployment of affected frameworks, evident in over 968,000 exposed instances, the window for both opportunistic and targeted attacks remains wide.

IOCs

PolySwarm has multiple samples associated with exploitation of CVE-2025-55182.

EtherRAT

E38362aca79b16d588174e64a33cc688504c845d882624243fde90abd578bd7d

Click [here](#) to view all samples of EtherRAT in our PolySwarm portal.

NoodleRAT

33641bfbbdd5a9cd2320c61f65fe446a2226d8a48e3bd3c29e8f916f0592575f

Click [here](#) to view all samples of NoodleRAT in our PolySwarm portal.

SNOWLIGHT

a455731133c00fdd2a141bdfba4def34ae58195126f762cdf951056b0ef161d4

1663d98c259001f1b03f82d0c5bee7cfd3c7623ccb83759c994f9ab845939665

55ae00bc8482afd085fd128965b108cca4adb5a3a8a0ee2957d76f33edd5a864

62e9a01307bcf85cdaeeccaf6efb5be72a622c43a10f06d6d6d3b566b072228d

7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a

Click [here](#) to view all samples of SNOWLIGHT in our PolySwarm portal.

VShell

4a759cbc219bcb3a1f8380a959307b39873fb36a9afd0d57ba0736ad7a02763b

Click [here](#) to view all samples of VShell in our PolySwarm portal.

Mirai

7e0a0c48ee0f65c72a252335f6dcd435dbd448fc0414b295f635372e1c5a9171

8067c9bf0ca1a67352fc7b8c9cc99fed8d9f3f57246712a6cd692edc4b66d323

aa315ec8f84aa33b84b7c920cb9b9f91a5485321ce16d198efec1abc604f8e3a

858874057e3df990ccd7958a38936545938630410bde0c0c4b116f92733b1ddb

8067c9bf0ca1a67352fc7b8c9cc99fed8d9f3f57246712a6cd692edc4b66d323

aa315ec8f84aa33b84b7c920cb9b9f91a5485321ce16d198efec1abc604f8e3a

858874057e3df990ccd7958a38936545938630410bde0c0c4b116f92733b1ddb

Click [here](#) to view all samples of Mirai in our PolySwarm portal.

Don't have a PolySwarm account? Go [here](#) to sign up for a free Community plan or subscribe.

Contact us at hivemind@polyswarm.io | Check out our [blog](#) | [Subscribe](#) to our reports.

Topics: [Threat Bulletin](#), [Linux backdoor](#), [post-exploitation activity](#), [CVE-2025-55182](#), [React RCE](#), [Next.js vulnerability](#), [KSwapDoor backdoor](#), [Cobalt Strike Linux](#), [EtherRAT](#)



Source: <https://blog.polyswarm.io/multiple-threat-actors-leveraging-cve-2025-55182-react2shell>