# AL2026_12 React2Shell Exploited in Automated Credential Theft Campaign (April 10th, 2026)

## Description

Security researchers have identified a large-scale cyber campaign exploiting the **React2Shell** vulnerability to automate credential theft from vulnerable web applications built with React and Next.js frameworks.

The vulnerability, tracked as **CVE-2025-55182**, is a critical remote code execution (RCE) flaw that allows attackers to execute arbitrary commands on servers running vulnerable React Server Components implementations. Threat actors are actively exploiting this flaw to compromise cloud-hosted web applications and extract sensitive data, including database credentials, API keys, and cloud access tokens.

Due to the widespread use of React and Next.js in modern web development, organizations operating cloud-based applications may be at risk if their systems are not updated to patched versions.

## Attack Details

The attack campaign leverages the React2Shell vulnerability to gain unauthorized access to application servers and automate the extraction of sensitive credentials.

Key characteristics include:

- **Vulnerability:** CVE-2025-55182 – a critical remote code execution vulnerability affecting React Server Components and frameworks such as Next.js.
- **Unauthenticated exploitation:** Attackers can trigger the vulnerability by sending specially crafted HTTP requests that exploit insecure deserialization within the React Server Components “Flight” protocol.
- **Automated credential harvesting:** Compromised systems are used to collect database credentials, AWS keys, SSH private keys, API tokens, and other environment secrets stored on servers.
- **Use of automation frameworks:** The attackers deploy an automated framework known as **NEXUS Listener** to manage compromised hosts and aggregate stolen data from multiple victims.

- **Large-scale compromise:** Researchers observed hundreds of compromised hosts across multiple cloud providers and regions, demonstrating the widespread exploitation of the vulnerability.
- **Threat actor tracking:** Cisco Talos attributes the activity to a threat cluster identified as **UAT-10608**, which is associated with automated credential harvesting operations.

Because modern web applications frequently store sensitive configuration data in environment variables, successful exploitation can expose credentials that enable attackers to move laterally across cloud infrastructure.

## Remediation

Organizations using React-based web applications should take the following actions immediately:

- **Apply security updates:** Upgrade React, Next.js, and related packages to patched versions that address CVE-2025-55182.
- **Rebuild and redeploy applications:** After updating dependencies, rebuild applications and redeploy them to ensure vulnerable components are removed from production environments.
- **Secure environment secrets:** Avoid storing sensitive credentials in plaintext environment variables and use secure secrets-management systems instead.
- **Monitor server logs:** Review application logs for unusual HTTP requests, command execution attempts, or unauthorized access to environment files.
- **Implement Web Application Firewall (WAF) protections:** Configure WAF rules capable of detecting malicious requests targeting React Server Components endpoints.
- **Rotate compromised credentials:** If exploitation is suspected, immediately rotate all potentially exposed database credentials, API keys, cloud tokens, and SSH keys.
- **Continuous vulnerability scanning:** Implement automated dependency scanning tools to detect vulnerable open-source libraries within development pipelines.
- **Security monitoring:** Deploy intrusion detection and monitoring tools to detect abnormal server behavior and suspicious outbound connections from application servers.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

## References

- Toulas, B. (2026). *Hackers exploit React2Shell in automated credential theft campaign.* Retrieved from BleepingComputer:

https://www.bleepingcomputer.com/news/security/hackers-exploit-react2shell-in-automated-credential-theft-campaign/