Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

React2STEAL: Hijacked GitHub Actions Fuel React2Shell Credential Theft

Date of Publication	Admiralty Code	TA Number
November 20, 2026	A1	TA2026348

Summary

First Seen: October 2026

Targeted Regions: Worldwide

Targeted Platforms: Linux, Cloud (AWS, GCP, Azure), Kubernetes, GitHub Actions

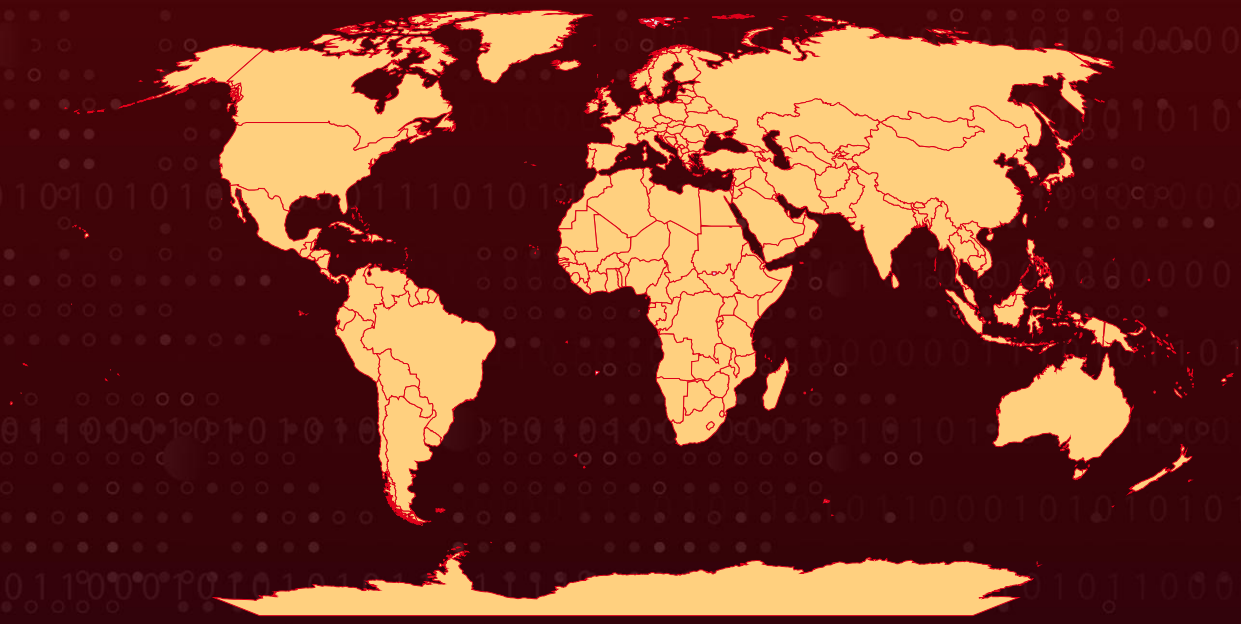
Targeted Products: Meta React Server Components, Vercel Next.js

Campaign Name: React2STEAL

Malware: fast_recon.js (JavaScript credential stealer)

Attack: React2STEAL is an unattributed campaign that turns 45 hijacked GitHub repositories into a free, distributed exploitation platform. GitHub Actions workflows mass-scan for Next.js servers, exploit React2Shell (CVE-2025-55182) and the Next.js middleware bypass (CVE-2025-29927), then run fast_recon.js inside the victim's Node.js process. The payload pulls IAM credentials through SSRF to the cloud metadata service, validates stolen AI provider keys against live APIs, and commits the loot back to the same public repositories. At least 1,281 hostnames across about 1,100 domains are compromised.

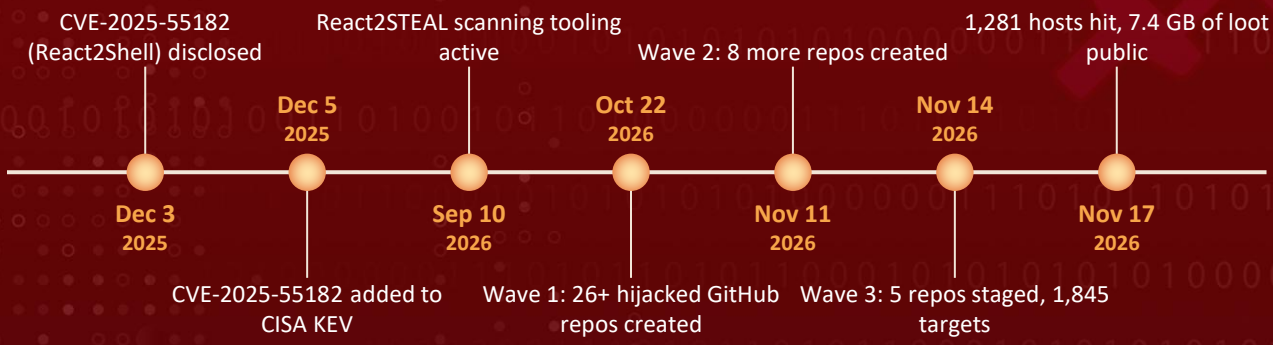
Attack Regions



Targeted Non-Targeted

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Timeline



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55182	React2Shell (React Server Components Remote Code Execution Vulnerability)	Meta React Server Components	✗	✓	✓
CVE-2025-29927	Next.js Middleware Authorization Bypass Vulnerability	Vercel Next.js	✗	✗	✓

Attack Details

#1 React2STEAL runs from 45 public GitHub repositories named ci-wk-{number}, owned by 44 accounts; of 26 profiles reviewed, 20 had no followers. The account owners appear to be victims rather than operators, and how their tokens were stolen is not established. The repositories were created in three waves on October 22, November 11 and November 14, 2026, with code comments dating back to September 10, 2026.

#2 Initial access comes from exploiting React2Shell (CVE-2025-55182), a CVSS 10.0 pre-authentication remote code execution flaw caused by prototype chain pollution in the React Server Components Flight protocol. The scanner also probes for CVE-2025-29927, a Next.js middleware authorization bypass triggered via the x-middleware-subrequest header.

#3 Each run starts when the operator commits a list of 20,000 hostnames and dispatches a GitHub Actions scan workflow on an ubuntu-latest runner with a 350-minute timeout. prefilter_nextjs.py narrows the list to probable Next.js hosts at a concurrency of 400, then batch_output.py fires seven React2Shell request variants, each built to evade WAF signatures.

#4 On success, the JavaScript KIT payload fast_recon.js runs inside the victim's Node.js process. It installs nothing, downloads no second stage and sets no persistence. It harvests environment variables, host and network details, cloud credential files, Kubernetes service account tokens and .env files, and a variant added on October 23, 2026 captures full configuration file contents.

#5 In parallel, batch_output.py abuses the Next.js /_next/image endpoint as an SSRF primitive to reach the instance metadata service at 169.254.169.254 and pull IAM role credentials. The payload also checks 28 environment variable names across ten AI providers, including OpenAI, Anthropic and Gemini, and validates each stolen key through live inference calls capped at 20 tokens.

#6 Exfiltration uses GitHub itself as the drop site. Results are committed and pushed to the same public repository as plaintext, JSON and ZIP files, and the push step runs unconditionally so partial results are never lost. A Telegram delivery path with a hard-coded bot token exists but is disabled by default.

#7 Roughly 7.4 GB of stolen data, including more than 9,100 ZIP archives, has been committed publicly, exposing secrets of organizations from small firms to large institutions, often via dev, staging and admin hosts. As of November 17, 2026, new results were landing about every 11 minutes, and because clones, forks and Git history keep the data, deleting the repositories does not remediate the exposure.

Recommendations

Patch React Server Components and Next.js: Upgrade the react-server-dom packages to 19.0.3, 19.1.4, 19.2.3 or later, and move Next.js to a release patched for both CVE-2025-55182 and CVE-2025-29927 (such as 15.5.7 or 16.0.7 and later).

- **Strip the x-middleware-subrequest Header at the Edge:** Until every Next.js deployment is patched, configure the reverse proxy, load balancer or WAF to drop inbound requests carrying the x-middleware-subrequest header.
- **Deploy React2Shell Detection Signatures:** Block POST requests with a Next-Action: x header and a multipart boundary containing bissa_cve_boundary, abnormal padding, or null bytes in the Content-Type header.
- **Rotate Every Secret Reachable by Affected Servers:** On any exposed host, rotate environment and .env secrets, database credentials, Stripe keys, Kubernetes tokens, cloud IAM credentials and AI provider keys.
- **Enforce IMDSv2 and Restrict Metadata Access:** Require IMDSv2 session tokens on AWS instances and apply equivalent metadata hardening on GCP and Azure so that SSRF requests cannot retrieve instance role credentials.
- **Contain Hijacked GitHub Accounts:** Treat any account hosting matching artifacts as compromised: revoke tokens, SSH keys and OAuth grants, reset credentials and enforce phishing-resistant MFA.
- **Restrict GitHub Actions Usage and CI Egress:** Set default workflow token permissions to read-only, limit which workflows may run, and restrict runner egress to approved destinations.

Detection Rules

Suricata rules | React2Shell exploit, Next.js middleware bypass and metadata SSRF

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"HiveForce React2STEAL React2Shell CVE-2025-55182 Exploit Attempt"; flow:established,to_server; http.method; content:"POST"; http.header; content:"Next-Action|3a 20|x"; nocase; http.request_body; content:"bissa_cve_boundary"; reference:cve,2025-55182; classtype:web-application-attack; sid:9202601; rev:1;)

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"HiveForce Next.js Middleware Bypass CVE-2025-29927 Attempt"; flow:established,to_server; http.header_names; content:"x-middleware-subrequest"; nocase; reference:cve,2025-29927; classtype:web-application-attack; sid:9202602; rev:1;)

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"HiveForce React2STEAL Next.js Image SSRF to Cloud Metadata"; flow:established,to_server; http.uri; content:"/_next/image"; content:"169.254.169.254"; distance:0; classtype:web-application-attack; sid:9202603; rev:1;)
```

YARA rule | React2STEAL scanner scripts and fast_recon.js stealer

```
rule HiveForce_React2STEAL_Tooling {
  meta:
    description = "Detects React2STEAL scanner scripts and fast_recon.js stealer"
    author = "Hive Pro"
    date = "2026-11-20"
  strings:
    // Scanner and exploit strings
    $s1 = "bissa_cve_boundary"
    $s2 = "x-middleware-subrequest"
    $s3 = "SEND_TELEGRAM"
    $s4 = "SCAN_REGISTRY_DB"
    $s5 = "PREFILTER_RETRY_CONCURRENCY"
    $s6 = "meta-data/iam/security-credentials"
    $s7 = "vulnerables/valid_target_"
    // fast_recon.js stealer and AI key validation strings
    $r1 = "secret_files"
    $r2 = "OPENROUTER_API_KEY"
    $r3 = "DEEPSEEK_API_KEY"
    $r4 = "DASHSCOPE_API_KEY"
    $r5 = "NEXT_PUBLIC_OPENAI_API_KEY"
    $r6 = "claude-3-5-haiku-latest"
  condition:
    filesize < 2MB and (3 of ($s*) or 4 of ($r*))
}
```

Sigma rule | Node.js process reading cloud and Kubernetes credentials (EDR)

```
title: Node.js Process Reading Cloud or Kubernetes Credentials
id: 2da448ca-9160-4007-ac57-b8e411658ac4
description: Detects React2STEAL fast_recon.js reading cloud and Kubernetes credentials
author: Hive Pro
date: 2026-11-20
tags: [attack.credential-access, attack.t1552.001]
logsource:
  product: linux
  category: file_access
detection:
  selection_process:
    Image|endswith: '/node'
  selection_files:
    TargetFilename|contains:
      - '/var/run/secrets/kubernetes.io/serviceaccount/token'
      - '/.aws/credentials'
      - '/.config/gcloud/'
      - '/.azure/'
      - '/.env'
  condition: all of selection_*
falsepositives:
  - Node.js applications that legitimately use cloud SDKs or Kubernetes clients
level: high
```

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Resource Development	T1584: Compromise Infrastructure	T1584.006: Web Services
	T1608: Stage Capabilities	T1608.001: Upload Malware
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Defense Evasion	T1036: Masquerading	
Discovery	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
	T1049: System Network Connections Discovery	
	T1057: Process Discovery	
	T1083: File and Directory Discovery	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files T1552.005: Cloud Instance Metadata API
Collection	T1005: Data from Local System	

Tactic	Technique	Sub-technique
Collection	T1560: Archive Collected Data	
Command and Control	T1102: Web Service	
Exfiltration	T1567: Exfiltration Over Web Service	T1567.001: Exfiltration to Code Repository

Indicators of Compromise (IOCs)

TYPE	VALUE
Git Object ID	ee6e5addfe591923fc385553cb66cf0d25634a6b, 823e8824acb61aa036a3e0c8945a63d4a2e0cf64, 418bf778648c9f5fa4fd95340e07a05dca797e37, fda8b5097a5223a5afcbc0c346a8af55faa4fd07
IPv4	156[.]67[.]221[.]96
Filename	scan.yml, prefilter_nextjs.py, batch_output.py, fast_recon.js, wfx-audit.md, scanned.db, scan_00.db, scan_01.db, cands_00.txt, cands_01.txt, pf_00.err, pf_01.err, scan_00.log, scan_01.log, hosts_{date}_{time}.txt

TYPE	VALUE
File Path	.github/workflows/scan.yml, bin/prefilter_nextjs.py, bin/batch_output.py, bin/fast_recon.js, docs/wfx-audit.md, vulnerables/valid_target_{host}_{timestamp}.txt
HTTP Request	Next-Action: x (multipart boundary containing bissa_cve_boundary), x-middleware-subrequest header repeated five times, /_next/image?url= targeting 169[.]254[.]169[.]254 (meta-data/iam/security-credentials/)
User Agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
GitHub Account	dascxzcw
GitHub Repository	ci-wk-{number}
Git Branch	wfx-docs, ci-sync-{6 characters}

Patch Links

CVE-2025-55182: https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

CVE-2025-55182: https://nextjs.org/blog/CVE-2025-66478

CVE-2025-29927: https://github.com/vercel/next.js/security/advisories/GHSA-f82v-jwr5-mffw

References

https://opensourcemalware.com/blog/react2steal-github-actions

https://www.hivepro.com/threat-advisory/nextjs-under-siege-as-cve-2025-29927-opens-the-floodgates-for-attackers

https://www.hivepro.com/threat-advisory/react2shell-flaw-in-react-server-components-under-active-attack

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 Demo of **HivePro**.

REPORT GENERATED ON

November 20, 2026 • 8:10 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com