pellera

THREAT INTEL REPORT 2025

Prepared by: Pellera Threat Intel Team
pellera.com | 800.747.8585

DECEMBER

Driving Momentum. Accelerating Change. Empowering IT Transformation.

Pellera Technologies was born out of the combined expertise of Converge Technology Solutions and Mainline Information Systems, two industry leaders with over 35+ years of experience and a shared vision for innovation. Together, we empower businesses to achieve greater efficiency, adaptability, and growth for today and tomorrow.

Our commitment is to reshape what's possible with IT, offering advanced solutions in digital infrastructure, cloud, cybersecurity, and AI. We don't just deliver technology—we partner with you to build tailored strategies designed to simplify complexities, unlock opportunities, and drive transformational outcomes.

At Pellera, momentum builds here through collaborative, people-first technology designed to fuel progress and deliver measurable impact.

pellera

CONVERGE TECHNOLOGY SOLUTIONS + Mainline®

Observations for

December 2025

Activity observed this month reinforced how quickly technical exposure can translate into operational risk when widely adopted platforms or services are involved. The emergence of **React2Shell** demonstrated how a single vulnerability in a modern application framework can place entire web application tiers at risk within days, not weeks. Exploitation rapidly evolved from broad scanning into targeted access attempts focused on persistence, credential exposure, and follow-on abuse of cloud environments. The pace of exploitation highlighted ongoing gaps between vulnerability disclosure, patch deployment, and runtime visibility across internet-facing applications.

In parallel, Russian state-sponsored and aligned activity continued to favor reliability and scale over technical novelty. Rather than relying on new exploits, **GRU-linked actors** and affiliated hacktivist groups focused on abusing misconfigured edge devices, cloud appliances, and exposed remote management services. This approach enabled consistent access across critical infrastructure and cloud-hosted environments while reducing the likelihood of detection. The targeting of operational technology environments through exposed interfaces further blurred the line between cyber activity and physical risk, particularly where remote access controls and monitoring were weak.

Together, these developments point to a sustained emphasis on exploiting trust—whether embedded in application frameworks, cloud configurations, or perimeter infrastructure. **The threat landscape continues to reward attackers who can move quickly against known weaknesses and leverage them at scale.** Organizations with limited visibility into application behavior, credential use, and edge exposure remain most at risk, particularly where ownership between development, infrastructure, and security teams is fragmented.

Executive Overview

REACT2SHELL

Audience

- CISO
- Project Managers
- Cybersecurity Analysts
- Risk Management Professionals
- IT Managers

HIGH

RISK

GLOBAL

GEOGRAPHIC SCOPE

Any Sector Utilizing React

BUSINESS IMPACT

React2Shell (CVE-2025-55182) enabled unauthenticated remote code execution against widely deployed React and Next.js applications, creating immediate risk to web application tiers and associated cloud credentials. Exploitation activity rapidly transitioned from scanning to persistent access and monetization, increasing exposure to credential theft, lateral movement, and service disruption. Organizations operating internet-facing RSC-enabled applications faced elevated risk during early December 2025, particularly where patching, runtime telemetry, and egress controls lagged disclosure timelines.

READ MORE: REACT2SHELL

GRU & CLOUD MISCONFIGURATIONS

Audience

- CISO
- IT Operations Managers & Teams
- Risk Management Professionals
- Security Operations Team
- IT Security Managers
- Incident Response Teams
- System Administrators

HIGH

RISK

GLOBAL

GEOGRAPHIC SCOPE

Global Infrastructure, Government, and Cloud-Hosted Services

INDUSTRY IMPACT

Russian state-sponsored actors and affiliated hacktivist groups have intensified campaigns against critical infrastructure across the U.S., Europe, and the Middle East. Recent findings reveal a tactical shift from zero-day exploitation to the abuse of misconfigured network edge devices such as routers, VPN concentrators, and cloud-hosted appliances.

This shift, attributed to GRU-linked groups including Sandworm (APT44), enables stealthier and more scalable access. Simultaneously, pro-Russia hacktivists have targeted operational technology (OT) environments via exposed VNC interfaces, posing direct threats to public safety and operational continuity. These campaigns underscore a pressing need for rigorous edge hardening, credential protection, and cross-sector collaboration.

READ MORE: GRU & CLOUD MISCONFIGURATIONS

REACT2SHELL

Overview & Impact

React2Shell exploited unsafe deserialization during server-side reconstruction of React component trees. React Server Components were not designed to process untrusted input, allowing malformed Flight payloads to influence execution flow prior to authentication. Default framework configurations exposed this attack surface without requiring application-specific misconfiguration.

- **Confidentiality Impact**
  - Successful exploitation enabled attackers to execute arbitrary code within the application runtime, granting access to environment variables, application secrets, and embedded credentials accessible to the Node.js process.
  - In cloud-hosted deployments, compromised runtimes frequently possessed access to cloud IAM credentials, API tokens, or service account keys, increasing the likelihood of credential harvesting.
  - Exposure extended beyond the application layer where runtimes were permitted to query cloud metadata services, secret management APIs, or internal microservices, enabling downstream data access.
- **Integrity Impact**
  - Attackers were able to modify application hosts by writing files, installing tooling, or altering startup configurations following exploitation.
  - Post-exploitation activity included deployment of backdoors, reverse proxies, and custom Linux implants, creating sustained unauthorized access.
  - Where CI/CD artifacts or build credentials were accessible, exploitation introduced risk of application tampering or supply chain contamination, particularly in environments with shared build pipelines.
- **Availability Impact**
  - Opportunistic campaigns deployed cryptominers and resource-intensive tooling, degrading application performance and increasing infrastructure costs.
  - Emergency mitigations and uncoordinated patching introduced service instability in some environments, including partial outages and degraded response times.
  - Incident response activities, including forced redeployments and credential rotation, resulted in planned and unplanned downtime for affected services.
- **Operational Impact**
  - Organizations lacking runtime telemetry experienced delayed detection, allowing attackers to maintain access beyond initial exploitation.
  - Incident response required coordination across application teams, cloud operations, and security, diverting resources from planned development and operational initiatives.
  - Environments treating the issue as a patch-only vulnerability faced increased remediation effort when post-exploitation artifacts were later discovered.
- **Business and Financial Impact**
  - Exposure of sensitive data and credentials increased the risk of data breach notifications, customer impact, and reputational damage.
  - Infrastructure misuse through cryptomining and persistent access increased cloud consumption costs.
  - Extended remediation efforts, forensic analysis, and external response support generated unplanned operational expense.

- **Regulatory and Compliance Impact**
    - Confirmed exploitation involving access to personal, customer, or regulated data triggered breach assessment and reporting obligations under applicable regulatory frameworks.
    - Organizations operating in regulated sectors faced additional scrutiny regarding patch management timelines, logging sufficiency, and incident response effectiveness.
    - Inclusion of CVE-2025-55182 in CISA's Known Exploited Vulnerabilities catalog elevated compliance expectations for timely remediation in regulated and critical infrastructure environments.

Observations

- **CVE-2025-55182 (React2Shell)**
    - **Context:** Unauthenticated remote code execution via RSC Flight protocol deserialization
    - **Detection Priority:** Critical
    - **Expiration Likelihood:** Medium
    - Blocking Recommendation: Patch affected React and Next.js versions and redeploy applications
- **China-nexus exploitation infrastructure (4–5 December 2025)**
    - **Context:** Early exploit testing and scanning activity
    - **Detection Priority:** High
    - **Expiration Likelihood:** High
    - Blocking Recommendation: Monitor and alert on repeated malformed RSC requests and anomalous POST traffic
- **Iterative exploit debugging behavior**
    - **Context:** Repeated payload attempts and command execution validation
    - **Detection Priority:** High
    - **Expiration Likelihood:** Medium
    - Blocking Recommendation: Rate-limit and alert on repeated failed exploit signatures
- **Advanced Linux implants and tunneling tools**
    - **Context:** Persistence and access expansion following exploitation
    - **Detection Priority:** High
    - **Expiration Likelihood:** Medium
    - Blocking Recommendation: Hunt for unauthorized services, startup artifacts, and outbound tunnels

Guidance

Strategic Intelligence

- **Threat Actor Context**
    - China-nexus threat groups assessed as Earth Lamia and Jackpot Panda leveraged React2Shell within hours of disclosure.
    - Activity included shared anonymization infrastructure and repeated exploit attempts consistent with operational testing.
- **Trend Analysis**
    - Exploitation progressed rapidly from disclosure to automated scanning and sustained post-exploitation.
    - Payload diversity increased over time, indicating continued adversary investment.
- **Contextual Insight**
    - RSC-enabled applications often operate with elevated trust and access to internal services and secrets.
    - This positioning elevated React2Shell from a web application flaw to a cloud access risk.

- **Business Risk Mapping**
  - Highest exposure occurred in internet-facing Next.js App Router deployments on Kubernetes and managed PaaS platforms.
  - Risk increased where Node.js runtimes possessed permissive cloud IAM roles.
- **Predictive Analysis**
  - Exploitation activity is expected to persist until patch saturation is achieved.
  - Similar deserialization architectures are likely to be targeted in future campaigns.

Operational Intelligence

- **Threat Vectors**
  - Crafted HTTP POST requests targeting RSC-capable endpoints enabled unauthenticated server-side code execution.
- **Adversary Infrastructure Intelligence**
  - Early activity leveraged anonymized VPS infrastructure.
  - Advanced campaigns employed dynamic command-and-control resolution, including blockchain-based mechanisms.
- **Defense Effectiveness Assessment**
  - Rapid patching and redeployment significantly reduced exposure.
  - WAF controls mitigated opportunistic exploitation but did not prevent adapted hands-on-keyboard activity.
- **Monitoring & Detection Gaps**
  - Limited process telemetry on web servers delayed detection.
  - Unrestricted outbound egress enabled tunneling and persistent command-and-control.
- **Time Analysis**
  - Exploitation began on 4 December 2025.
  - Peak exposure occurred between 3–8 December 2025.
- **Response Actions**
  - Effective actions included patching, credential rotation, persistence hunting, and outbound traffic review.

Tactical Intelligence

- **Mitigation Strategies**
  - Immediate patching and redeployment of affected applications
  - Rotation of credentials accessible to application runtimes
  - Incident-driven threat hunting on web-tier hosts
- **Preventive Measures**
  - Reduction of RSC endpoint exposure
  - Enforcement of least privilege for Node.js runtimes
  - Acceleration of patch deployment pipelines
- **Detection Engineering Guidance**
  - Alert on Node.js processes spawning shells or system utilities
  - Detect repeated malformed RSC requests
  - Monitor for unauthorized outbound tunnels or proxy usage

Threat Hunting Hypotheses

React Server Component Exploitation Attempts

Hypothesis: React Server Components exploitation attempts occurred against internet-facing applications during early December 2025.

RETURN >>>

Investigation Steps

- Review web server and reverse proxy logs for HTTP POST requests targeting RSC-capable endpoints between 3–8 December 2025.
- Identify malformed or repeated requests containing server-action headers or anomalous payload structures consistent with React2Shell exploitation.
- Correlate request source IPs with known scanning behavior or rapid iteration indicative of exploit testing.
- Validate whether any requests resulted in abnormal application responses, crashes, or error patterns preceding compromise.

Node.js Runtime Post-Exploitation Activity

Hypothesis: Successful React2Shell exploitation resulted in abnormal child process creation from Node.js or Next.js application runtimes.

Investigation Steps

- Search EDR or host telemetry for Node.js processes spawning shells, interpreters, or system utilities (e.g., sh, bash, curl, wget).
- Identify execution of discovery commands (id, uname, whoami, env) originating from web application processes.
- Review process trees to confirm parent–child relationships between Node.js runtimes and spawned processes.
- Validate findings against baseline application behavior to rule out legitimate build or deployment activity.

Credential Access and Cloud Metadata Enumeration

Hypothesis: Compromised React application servers accessed cloud metadata services or secret repositories following exploitation.

Investigation Steps

- Inspect network logs for requests from web-tier hosts to cloud metadata IP addresses or internal secret management endpoints.
- Correlate access timestamps with confirmed or suspected exploitation activity.
- Review cloud audit logs for unexpected credential enumeration or token generation events.
- Confirm whether accessed credentials were subsequently used from new IP addresses or services.

Persistence Mechanisms on Linux Web Hosts

Hypothesis: React2Shell exploitation led to the establishment of persistence mechanisms on Linux-based web application hosts.

Investigation Steps

- Examine cron tables, systemd services, and startup scripts for recently created or modified entries.
- Search for newly created binaries or scripts in temporary, hidden, or non-standard directories.
- Inspect filesystem metadata for artifacts created shortly after suspected exploitation windows.
- Validate persistence artifacts against known deployment and configuration management baselines.

RETURN >>>

Unauthorized Outbound Tunneling and Command-and-Control

Hypothesis: Compromised React application servers established unauthorized outbound tunnels or command-and-control connections.

Investigation Steps

- Analyze network flow data for long-lived outbound connections from web-tier hosts to unapproved external destinations.
- Identify use of tunneling tools, reverse proxies, or uncommon protocols inconsistent with application requirements.
- Correlate outbound activity with process execution telemetry to identify responsible binaries.
- Confirm whether outbound connections persisted across restarts or redeployments.

Sources

- **Wiz: React2Shell (CVE-2025-55182): Critical React Vulnerability**
- **AWS: China-nexus cyber threat groups rapidly exploit React2Shell vulnerability**
- **Sysdig: Detecting React2Shell**
- **VulnCheck: React2Shell Variants & Exploit Ecosystem**
- **Logpoint: After React2Shell: Following the Attacker From Access to Impact**
- **Sysdig: EtherRAT – DPRK uses novel Ethereum implant in React2Shell attacks**
- **JFrog: React2Shell (CVE-2025-55182): Detection & Mitigation Guide – UPDATED**
- **Trend Micro: CVE-2025-55182 – React2Shell Analysis, Proof-of-Concept Chaos, and In-the-Wild Exploitation**
- **Qualys: React2Shell – Decoding CVE-2025-55182, the Silent Threat in React Server Components**
- **Huntress: PeerBlight Linux Backdoor Exploits React2Shell (CVE-2025-55182)**

GRU & CLOUD MISCONFIGURATIONS

Overview & Impact

Since 2021, Russian threat actors have demonstrated sustained interest in critical infrastructure sectors, evolving their tradecraft to exploit misconfigurations in externally facing devices. Amazon’s threat intelligence and joint government advisories (FBI, NSA, CISA) confirm that Russian GRU-affiliated groups increasingly avoid high-cost zero-day exploits in favor of insecure configurations — offering persistent, low-risk access to targeted environments.

Compromised systems include AWS-hosted EC2 appliances, VPN gateways, and OT interfaces used in water, energy, and telecom operations. In one common technique, actors captured credentials via packet-capture features on compromised edge devices, then conducted replay attacks to escalate within victim environments. Concurrently, hacktivist entities aligned with Russian state interests (e.g., CARR, NoName057(16)) have exploited exposed VNC services to disrupt HMI operations, disable alarms, and compromise ICS safety.

- **Confidentiality Impact**
  - Credential harvesting via packet-capture features enabled access to internal services.
  - Compromised systems included VPNs and EC2 instances with access to IAM credentials and internal cloud resources.
- **Integrity Impact**
  - Post-exploitation modifications allowed for credential replay, lateral movement, and configuration changes.
  - Attackers deployed backdoors and remote tunneling tools across cloud and on-prem environments.
- **Availability Impact**
  - Compromised OT environments experienced alarm suppression and visibility loss, disrupting HMI operations.
  - Recovery operations, including credential rotation and instance redeployment, introduced service delays.
- **Operational Impact**
  - Cross-domain compromise required coordinated IR across cloud, IT, and OT teams.
  - Post-exploitation persistence increased response complexity.
- **Business and Financial Impact**
  - Long-term unauthorized access exposed organizations to reputational and legal consequences.
  - Infrastructure misuse and incident response activities increased operational costs.
- **Regulatory and Compliance Impact**
  - Breaches affecting OT and ICS assets triggered regulatory attention across critical sectors.
  - CVEs and campaign activity tied to CISA alerts may influence compliance reviews.

Observations

- **Edge Device Exploitation**
  - **Context:** Abuse of misconfigured network appliances including Fortinet, Ivanti, and Cisco.
  - **Detection Priority:** High
  - **Blocking Recommendation:** Audit external interfaces, enforce MFA, restrict remote admin access.
- **Credential Replay via EC2 Appliances**
  - **Context:** Use of curl.exe and packet-capture tools to harvest and replay credentials.
  - **Detection Priority:** High
  - **Blocking Recommendation:** Disable packet-capture on appliances, monitor credential reuse.
- **Hacktivist Targeting of VNC Interfaces**
  - **Context:** Brute-force logins and alarm manipulation via exposed VNC (port 5900).
  - **Detection Priority:** High
  - **Blocking Recommendation:** Block external VNC access, monitor HMI behavior.
- **Cloud Metadata and Credential Access**
  - **Context:** Compromised runtimes accessed cloud metadata services.
  - **Detection Priority:** Medium
  - **Blocking Recommendation:** Restrict metadata access and monitor for suspicious requests.

Guidance

Strategic Intelligence

- **Threat Context**
  - GRU-linked APT44 (Sandworm) prioritizes stealthy access to reduce detection.
  - Hacktivists align loosely with Russian state objectives, targeting weakly secured OT assets

- **Trends Analysis**
  - Shift away from zero-days to misconfiguration abuse.
  - Replay attacks and credential theft have become preferred tactics.
- **Contextual Insight**
  - Edge devices are treated as blind spots in many cloud and hybrid environments.
  - Exploited assets frequently have overprivileged cloud access.
- **Business Risk Mapping**
  - Internet-facing EC2 appliances and legacy VPNs present the highest exposure.
  - Organizations with limited cloud configuration enforcement are most at risk.
- **Predictive Analysis**
  - These tactics are likely to persist and evolve as default appliance security remains inconsistent.

Operational Intelligence

- **Threat Vectors**
  - Misconfigured EC2 devices, VPN concentrators, and firewalls.
  - Credential replay using data from compromised network appliances.
- **Adversary Infrastructure**
  - Activity linked to Russian VPS services and obfuscated C2 infrastructure.
- **Defense Assessment**
  - MFA, strict role-based access, and interface isolation prove effective.
  - Traditional IDS/IPS fail to catch misconfiguration abuse without behavioral telemetry.
- **Monitoring & Detection Gaps**
  - Limited visibility in OT systems and cloud appliance logs.
  - Absence of runtime EDR in edge systems prolongs undetected access.
- **Time Analysis**
  - Campaigns observed from late 2021 to late 2025, increasing in complexity.
- **Response Actions**
  - **Key measures:** patching, MFA, credential rotation, full network audit.

Tactical Intelligence

- **Mitigation Strategies**
  - Enforce MFA across all internet-exposed services.
  - Patch and harden VPN/firewall appliances and cloud-hosted devices.
  - Rotate credentials used by compromised systems
- **Preventive Measures**
  - Restrict cloud metadata service access.
  - Implement network segmentation for OT and cloud access paths.
- **Detection Engineering**
  - Monitor VNC connections, port 5900 traffic, and repeated auth failures.
  - Alert on unusual use of curl.exe and packet-capture tools.
  - Detect identity replay and abnormal login patterns across cloud/OT systems.

RETURN >>>

Threat Hunting Hypotheses

Credential Harvesting and Replay via Edge Appliances

Hypothesis: Adversaries used packet-capture features on EC2 appliances to harvest credentials for replay across environments.

Investigation Steps

- Review EC2 appliances for custom scripts or traffic capture utilities.
- Correlate login attempts across identity providers with EC2 timelines.
- Identify reused credentials originating from appliance source IPs.

Unauthorized Access to OT via VNC Interfaces

Hypothesis: Hacktivist actors accessed OT systems through exposed VNC services to disrupt operations.

Investigation Steps

- Search for repeated external VNC connections to OT IPs.
- Review alarm system logs for manual resets or disablements.
- Correlate with brute-force attempts and weak/default credentials.

Cloud IAM Abuse Post Appliance Compromise

Hypothesis: Cloud-hosted devices compromised by misconfiguration were used to pivot into IAM services.

Investigation Steps

- Review access to metadata IPs (169.254.169.254) from compromised hosts.
- Check cloud audit logs for new API token issuance or credential escalation.
- Confirm timeline correlation between appliance compromise and IAM actions.

Sources

- **Cybersecurity Dive: Russian hackers target critical infrastructure, exploit energy sector edge devices**
- **Dark Reading: Hacktivists Target Critical Infrastructure**
- **GovInfoSecurity: Russia's GRU Tied to Critical Infrastructure Cloud Breaches**
- **SecurityWeek: Amazon: Russian Hackers Favor Misconfigurations in Infrastructure Attacks**

RETURN >>>

pellera

Contact the Pellera Threat Intel Group at getsecure@pellera.com

pellera.com

A PELLERA PODCAST

Edge of I.T.