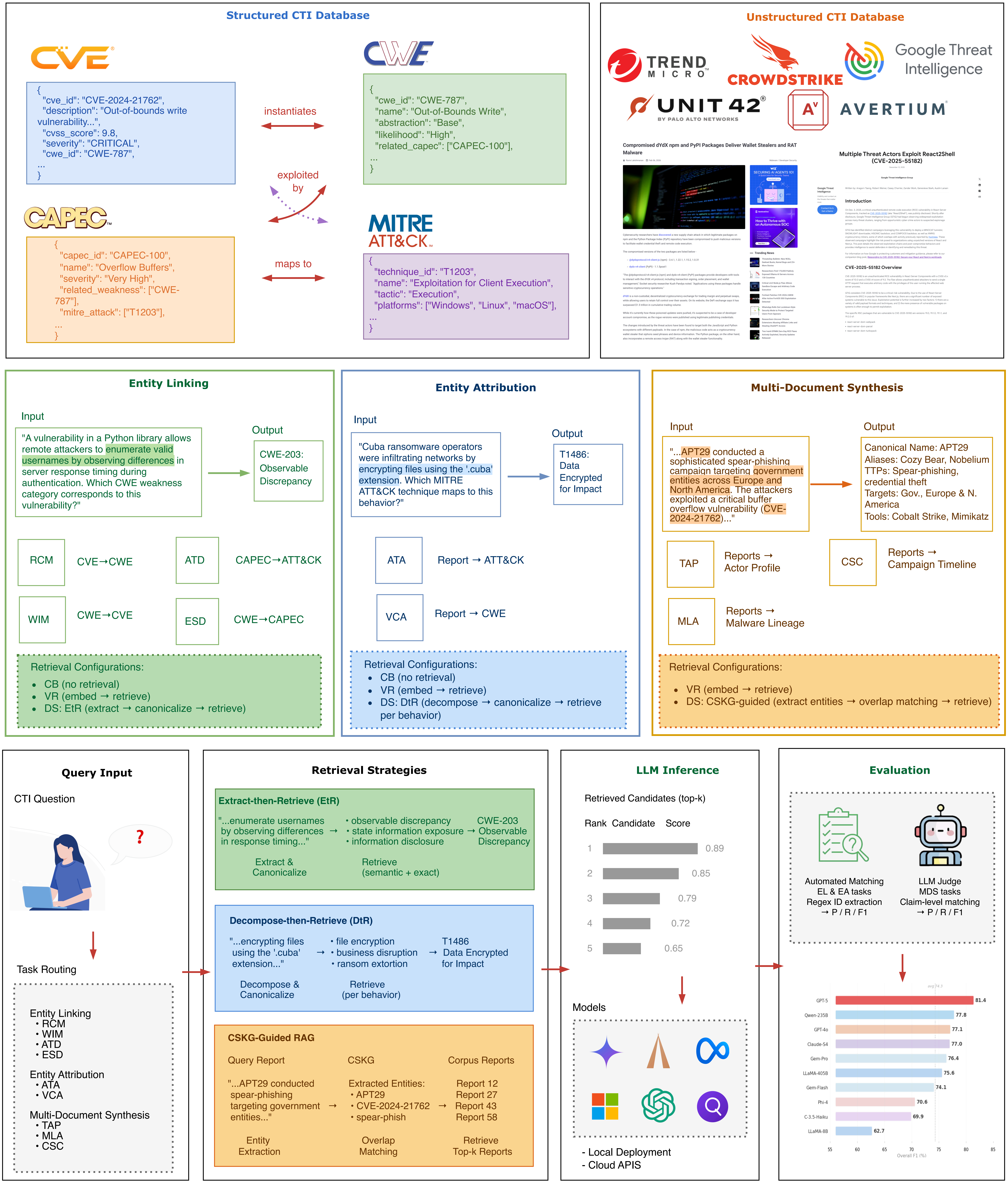

Structured CTI Database

```
{
  "cve_id": "CVE-2024-21762",
  "description": "Out-of-bounds write vulnerability...",
  "cvss_score": 9.8,
  "severity": "CRITICAL",
  "cwe_id": "CWE-787",
  ...
}
```

```
{
  "cwe_id": "CWE-787",
  "name": "Out-of-Bounds Write",
  "abstraction": "Base",
  "likelihood": "High",
  "related_capec": ["CAPEC-100"],
  ...
}
```

```
{
  "capec_id": "CAPEC-100",
  "name": "Overflow Buffers",
  "severity": "Very High",
  "related_weakness": ["CWE-787"],
  "mitre_attack": ["T1203"],
  ...
}
```

```
{
  "technique_id": "T1203",
  "name": "Exploitation for Client Execution",
  "tactic": "Execution",
  "platforms": ["Windows", "Linux", "macOS"],
  ...
}
```

Unstructured CTI Database

Compromised dYdX npm and PyPI Packages Deliver Wallet Stealers and RAT Malware

Ravie Lakshmanan Feb 06, 2026 Malware / Developer Security

Cybersecurity researchers have discovered a new supply chain attack in which legitimate packages on npm and the Python Package Index (PyPI) repository have been compromised to push malicious versions to facilitate wallet credential theft and remote code execution.

The compromised versions of the two packages are listed below -

- @dydxprotocol/v4-client-js (npm) - 3.4.1, 1.22.1, 1.15.2, 1.0.31
- dydx-v4-client (PyPI) - 1.1.5post1

"The @dydxprotocol/v4-client-js (npm) and dydx-v4-client (PyPI) packages provide developers with tools to interact with the dYdX v4 protocol, including transaction signing, order placement, and wallet management," Socket security researcher Kush Pandya noted. "Applications using these packages handle sensitive cryptocurrency operations."

dYdX is a non-custodial, decentralized cryptocurrency exchange for trading margin and perpetual swaps, while allowing users to retain full control over their assets. On its website, the DeFi exchange says it has surpassed $1.5 trillion in cumulative trading volume.

While it's currently how these poisoned updates were pushed, it's suspected to be a case of developer account compromise, as the rogue versions were published using legitimate publishing credentials.

The changes introduced by the threat actors have been found to target both the JavaScript and Python ecosystems with different payloads. In the case of npm, the malicious code acts as a cryptocurrency wallet stealer that siphons seed phrases and device information. The Python package, on the other hand, also incorporates a remote access trojan (RAT) along with the wallet stealer functionality.

WIZ SECURING AI AGENTS 101 A Quick Intro for Security Teams Download now

SentinelOne PRACTITIONER'S GUIDE How to Thrive with an Autonomous SOC
- Actionable Insights
- Industry Intelligence
- Practitioner Checklists
- Product Overviews

Read Now →

Trending News

- ThreatsDay Bulletin: New RCEs, Darknet Busts, Kernel Bugs and 25+ More Stories
- Researchers Find 175,000 Publicly Exposed Ollama AI Servers Across 130 Countries
- Critical vm2 Node.js Flaw Allows Sandbox Escape and Arbitrary Code Execution
- Fortinet Patches CVE-2026-24858 After Active FortiOS SSO Exploitation Detected
- WhatsApp Rolls Out Lockdown-Style Security Mode to Protect Targeted Users From Spyware
- Researchers Uncover Chrome Extensions Abusing Affiliate Links and Stealing ChatGPT Access
- Two Ivanti EPMM Zero-Day RCE Flaws Actively Exploited, Security Updates Released

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

December 12, 2025

Google Threat Intelligence Group

Google Threat Intelligence

Visibility and context on the threats that matter most.

Contact Us & Get a Demo

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

Entity Linking

Input

"A vulnerability in a Python library allows remote attackers to enumerate valid usernames by observing differences in server response timing during authentication. Which CWE weakness category corresponds to this vulnerability?"

Output

CWE-203: Observable Discrepancy

RCM	CVE→CWE	ATD	CAPEC→ATT&CK
WIM	CWE→CVE	ESD	CWE→CAPEC

Retrieval Configurations:
- CB (no retrieval)
- VR (embed → retrieve)
- DS: EtR (extract → canonicalize → retrieve)

Entity Attribution

Input

"Cuba ransomware operators were infiltrating networks by encrypting files using the '.cuba' extension. Which MITRE ATT&CK technique maps to this behavior?"

Output

T1486: Data Encrypted for Impact

ATA	Report → ATT&CK
VCA	Report → CWE

Retrieval Configurations:
- CB (no retrieval)
- VR (embed → retrieve)
- DS: DtR (decompose → canonicalize → retrieve per behavior)

Multi-Document Synthesis

Input

"...APT29 conducted a sophisticated spear-phishing campaign targeting government entities across Europe and North America. The attackers exploited a critical buffer overflow vulnerability (CVE-2024-21762)..."

Output

Canonical Name: APT29
Aliases: Cozy Bear, Nobelium
TTPs: Spear-phishing, credential theft
Targets: Gov., Europe & N. America
Tools: Cobalt Strike, Mimikatz

TAP	Reports → Actor Profile	CSC	Reports → Campaign Timeline
MLA	Reports → Malware Lineage		

Retrieval Configurations:
- VR (embed → retrieve)
- DS: CSKG-guided (extract entities → overlap matching → retrieve)

Query Input

CTI Question

Task Routing

Entity Linking
- RCM
- WIM
- ATD
- ESD

Entity Attribution
- ATA
- VCA

Multi-Document Synthesis
- TAP
- MLA
- CSC

Retrieval Strategies

Extract-then-Retrieve (EtR)

"...enumerate usernames by observing differences in response timing..." → • observable discrepancy • state information exposure • information disclosure → CWE-203 Observable Discrepancy

Extract & Canonicalize — Retrieve (semantic + exact)

Decompose-then-Retrieve (DtR)

"...encrypting files using the '.cuba' extension..." → • file encryption • business disruption • ransom extortion → T1486 Data Encrypted for Impact

Decompose & Canonicalize — Retrieve (per behavior)

CSKG-Guided RAG

Query Report		CSKG		Corpus Reports
"...APT29 conducted spear-phishing targeting government entities..."	→	Extracted Entities: • APT29 • CVE-2024-21762 • spear-phish	→	Report 12 Report 27 Report 43 Report 58
Entity Extraction		Overlap Matching		Retrieve Top-k Reports

LLM Inference

Retrieved Candidates (top-k)

Rank	Candidate	Score
1		0.89
2		0.85
3		0.79
4		0.72
5		0.65

Models

- Local Deployment
- Cloud APIS

Evaluation

Automated Matching
EL & EA tasks
Regex ID extraction
→ P / R / F1

LLM Judge
MDS tasks
Claim-level matching
→ P / R / F1