**Alexander Ticket**

\*QRadar ID:\* **55269**

\*Description\*

ET WEB\_SERVER ColdFusion componentutils access — Probe for /CFIDE/componentutils/ suggesting ColdFusion component reconnaissance/exploitation attempt.

\*Victim:\*

38.242.128.144 - <http://oldsystem.cydeosec.com>

*\* Encoded log:\**

*"\\/CFIDE\\/componentutils\\/"*

*\* Decoded log:\**

*"/CFIDE/componentutils/"*

\*ATTACKER INFO:\*

\*IP:\* 145.239.154.85 on port 49704

\*User Agent:\* ""Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36" — this string is consistent with a desktop Chrome 94 on Windows 10, but User-Agent headers are trivially spoofable. Treat this UA as **not** proof of a human browser; automated scanners and exploit tools commonly impersonate popular browsers to evade detection. "

\*ANALYST INVESTIGATION:\*

\*Virus Total Result:\* **[here|https://www.virustotal.com/gui/ip-address/145.239.154.85]**

\*Security Vendors' Analysis from Virus Total:\* **6/95 security vendors flagged this IP address as malicious and 2 flagged as suspicious**

****

\*Talos Intelligence:\*

\*REPUTATION DETAILS:\*

**Email Reputation: \*Neutral\***

**Web Reputation: \*Questionable\***

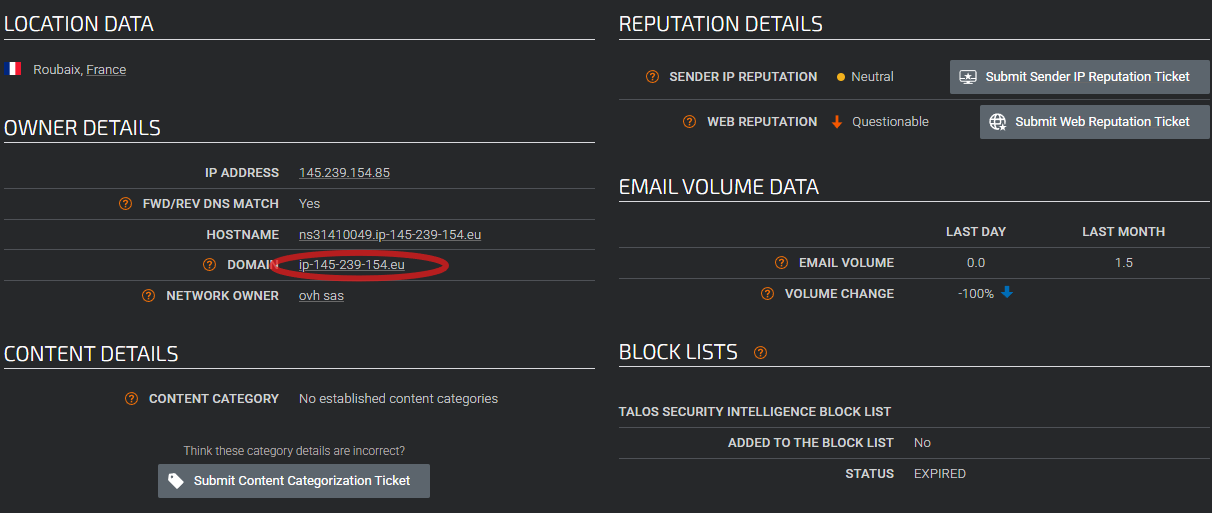
**\*BLOCK LISTS:\***

**\*Talos Security Intelligence Block List\***

**Added to the Block List = No**

**Status = EXPIRED**

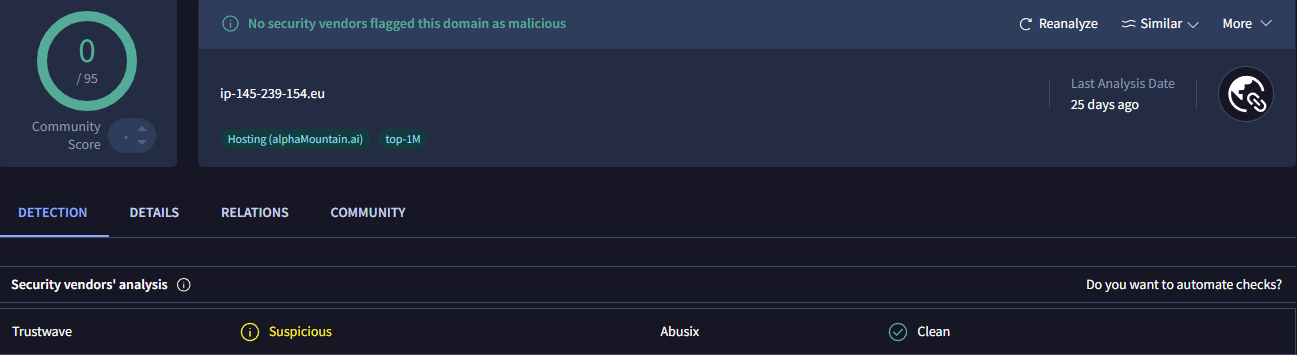
**\*Talos Result:\* [here|https://talosintelligence.com/reputation\_center/lookup?search=145.239.154.85]**

****

**The source IP \*\*145.239.154.85\*\* was checked in Cisco Talos, which resolved to the domain \*\*ip-145-239-154.eu\*\*.**

**A lookup of this domain in VirusTotal showed \*\*0/94 security vendors flagged it as malicious\*\*, but Trustwave flagged as "suspicious"**

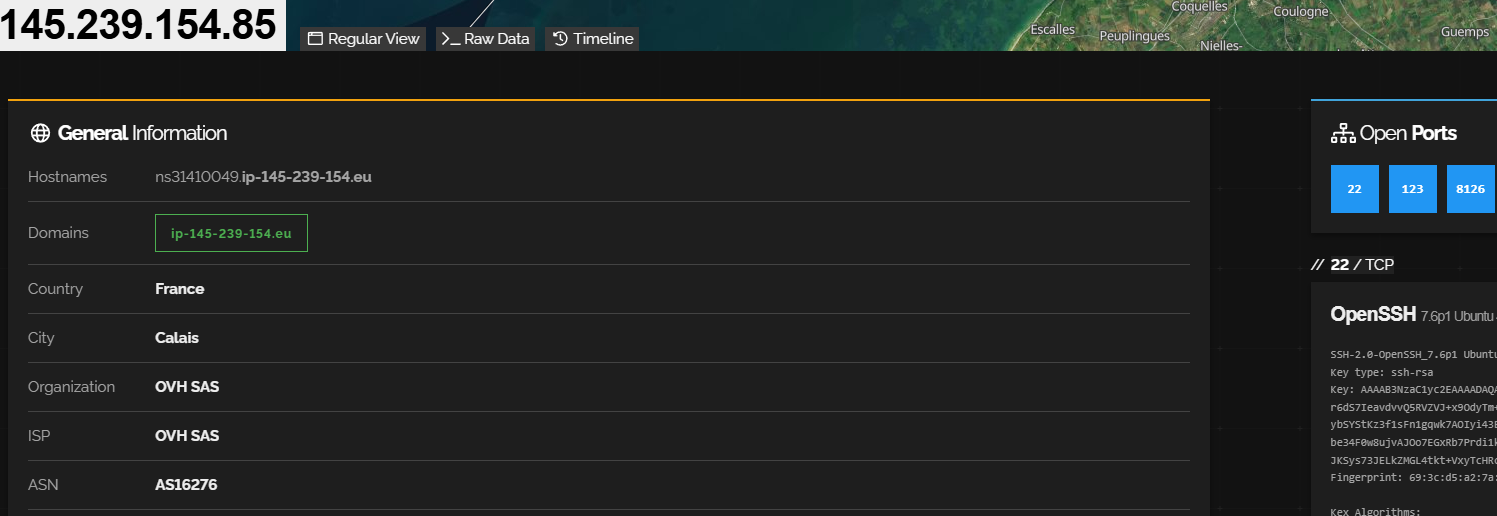
**[here|https://www.virustotal.com/gui/domain/ip-145-239-154.eu]**

****

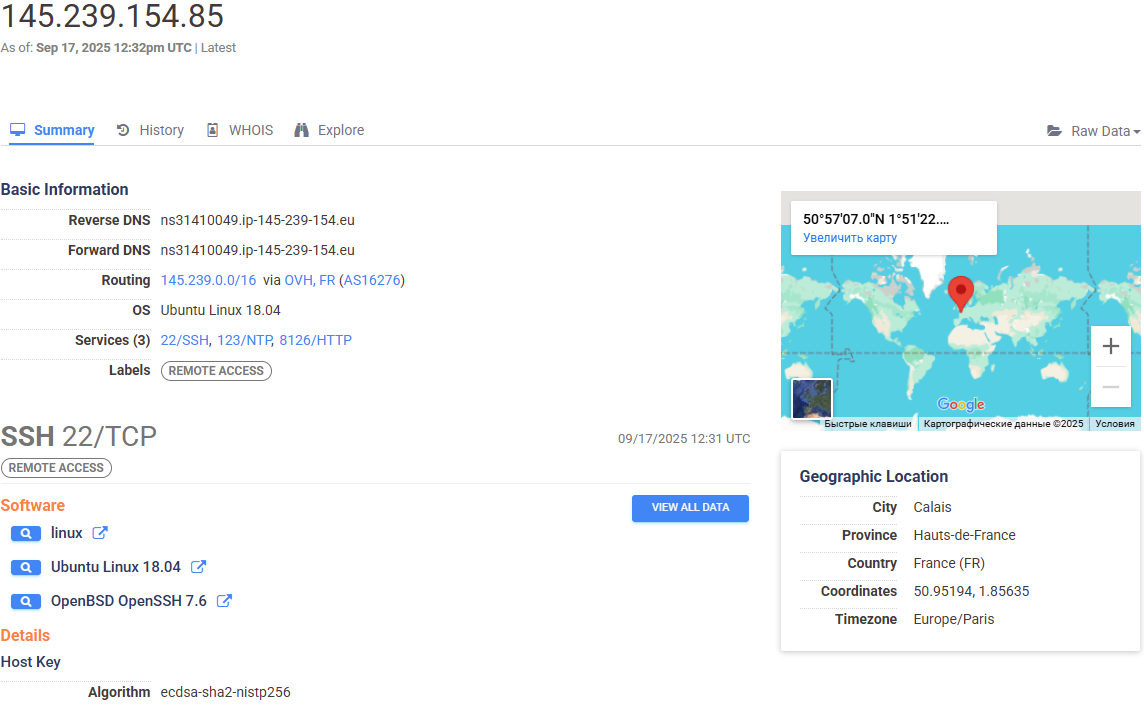
\*ShodanResult:\* **[here|https://www.shodan.io/host/145.239.154.85]**

\*Open Ports:\* 22, 123, 8126

|  |  |  |
| --- | --- | --- |
|  |  |  |

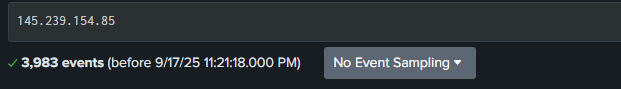
****

\*CensysResult:\* **[here|**https://search.censys.io/hosts/145.239.154.85**]**

****

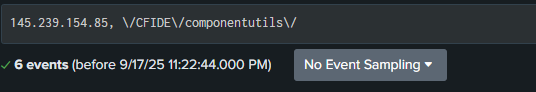
\*Splunk Investigation:\*A total of **3,983 events** were identified for IP 145.239.154.85.

To focus the investigation, the key URI \/CFIDE/componentutils\/ was applied, which reduced the dataset to **6 events**.



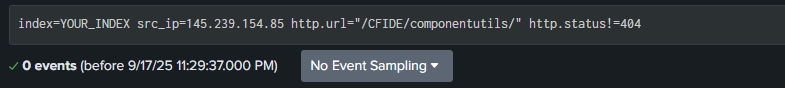
**↑↑↑**

**[Result1|https://splunk.cydeosec.com/en-US/app/search/search?earliest=0&latest=&q=search%20145.239.154.85&display.page.search.mode=smart&dispatch.sample\_ratio=1&sid=1758162216.120502]**



**↑↑↑**

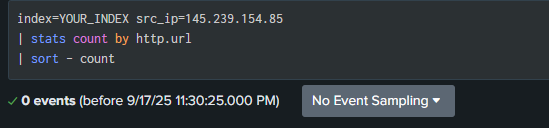
**[Result2|https://splunk.cydeosec.com/en-US/app/search/search?earliest=0&latest=&q=search%20145.239.154.85%2C%20%5C%2FCFIDE%5C%2Fcomponentutils%5C%2F&display.page.search.mode=smart&dispatch.sample\_ratio=1&sid=1758162236.120506]**



**↑↑↑**

**HTTP response status for all events: 404 (Not Found) – no successful exploitation observed.**

**[Result3|**https://splunk.cydeosec.com/en-US/app/search/search?earliest=0&latest=&q=search%20index%3DYOUR\_INDEX%20src\_ip%3D145.239.154.85%20http.url%3D%22%2FCFIDE%2Fcomponentutils%2F%22%20http.status!%3D404&display.page.search.mode=smart&dispatch.sample\_ratio=1&display.page.search.tab=events&display.general.type=events&sid=1758162577.120539**]**

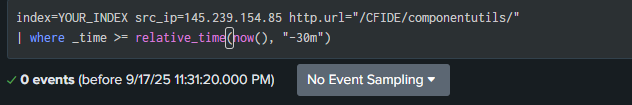


**↑↑↑**

**No additional URIs were found for IP 145.239.154.85.**

**This indicates the attacker focused only on /CFIDE/componentutils/ and did not attempt other paths.**

**[Result4|**https://splunk.cydeosec.com/en-US/app/search/search?earliest=0&latest=&q=search%20index%3DYOUR\_INDEX%20src\_ip%3D145.239.154.85%0A%7C%20stats%20count%20by%20http.url%0A%7C%20sort%20-%20count&display.page.search.mode=smart&dispatch.sample\_ratio=1&display.page.search.tab=statistics&display.general.type=statistics&sid=1758162625.120548**]**



**↑↑↑**

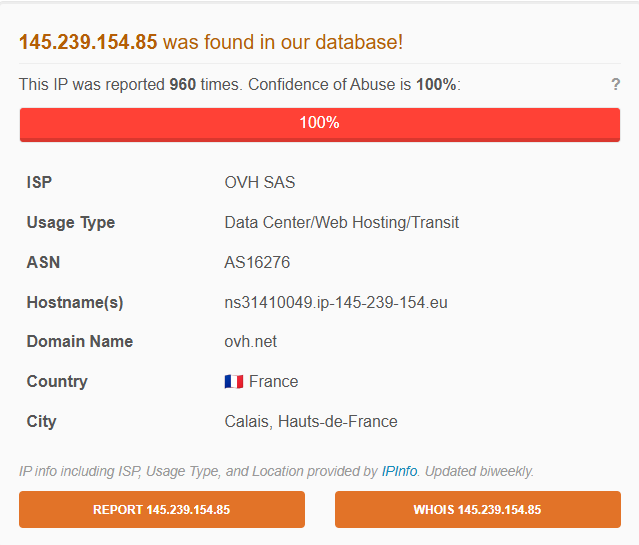
**No recent activity in the last 30 minutes, suggesting no ongoing attack.**

**[Result5|**https://splunk.cydeosec.com/en-US/app/search/search?earliest=0&latest=&q=search%20index%3DYOUR\_INDEX%20src\_ip%3D145.239.154.85%20http.url%3D%22%2FCFIDE%2Fcomponentutils%2F%22%0A%7C%20where%20\_time%20%3E%3D%20relative\_time(now()%2C%20%22-30m%22)&display.page.search.mode=smart&dispatch.sample\_ratio=1&display.page.search.tab=events&display.general.type=events&sid=1758162680.120555**]**

\*Raw Data:\*

*<168>suricata[8969]: {"timestamp":"2025-08-16T06:42:18.879129-0400","flow\_id":826671155015547,"in\_iface":"eth0","event\_type":"alert","src\_ip":"145.239.154.85","src\_port":49704,"dest\_ip":"38.242.128.144","dest\_port":80,"proto":"TCP","tx\_id":0,"alert":{"action":"allowed","gid":1,"signature\_id":2016182,"rev":6,"signature":"ET WEB\_SERVER ColdFusion componentutils access","category":"Web Application Attack","severity":1},"http":{"hostname":"vmi919546.contaboserver.net","url":"\/CFIDE\/componentutils\/","http\_user\_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/94.0.4606.81 Safari\/537.36","http\_content\_type":"text\/html","http\_method":"GET","protocol":"HTTP\/1.1","status":404,"length":289}}*

\*Additional Findings:\*



This IP address has been reported a total of **960** times from 312 distinct sources. 145.239.154.85 was first reported on July 27th 2024, and the most recent report was **42 minutes ago**.

\***ResultAbuseIPDB:\* [here|https://www.abuseipdb.com/check/145.239.154.85]**

**ANALYST ASSESSMENT**

**Summary:** Suricata detected ET WEB\_SERVER ColdFusion componentutils access from source IP **145.239.154.85** against 38.242.128.144 (oldsystem.cydeosec.com). Splunk shows **3,983** total events from this IP; filtering to the ColdFusion path /CFIDE/componentutils/ reduced the set to **6 events**. All six returned **HTTP 404 (Not Found)**. No other URIs or non-404 responses were observed. Overall, activity is consistent with automated reconnaissance rather than a successful exploit.

**Attack details:**

* **Source:** 145.239.154.85 (src port 49704) → **Destination:** 38.242.128.144:80
* **Targeted path:** /CFIDE/componentutils/ (Adobe ColdFusion component probe)
* **Events:** 6 requests to that path (subset of 3,983 total events from this IP)
* **HTTP status:** 404 for all observed attempts — **no successful response** recorded
* **Suricata signature:** ET WEB\_SERVER ColdFusion componentutils access (sid: 2016182 rev:6)

**Path breakdown / what it means:**

* /CFIDE/ — ColdFusion administrative/utility components commonly probed by attackers.
* componentutils — frequently targeted ColdFusion component; existence may allow remote actions or information disclosure if vulnerable.
* Observed requests appear to be **probes** to detect presence of ColdFusion endpoints; 404 responses indicate the path was not present/accessible.

**Method / Indicators:**

* **HTTP method:** GET — passive probing to discover endpoint.
* **User-Agent:** "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36" — looks like a common browser UA but is trivially spoofable; treat as **not** proof of human browsing.
* **Timing/volume:** large number of events from the source overall (3.98k) but only 6 hits to the specific ColdFusion path — typical scanner behavior.

**Threat Intelligence enrichment :**

* **VirusTotal (IP):** 6/95 vendors flagged the IP as malicious; 2 vendors flagged as suspicious.
* **VirusTotal (domain ip-145-239-154.eu):** 0/94 detections for the domain itself, but Trustwave labeled it **suspicious**.
* **Talos:** reputation lookup shows *no active block list entry / status: EXPIRED* (no current block).
* **Shodan:** host shows open ports including 22, 123, 8126 (note: presence of open services increases attack surface).
* **AbuseIPDB:** IP reported ~**960** times from **312** distinct sources (historical abuse reports).
* **Censys / other scanners:** present (links saved in ticket for analysts to review full host/service fingerprint).

Note: TI sources are discordant — some vendors flag the IP, domain VT shows 0/94 but Trustwave marks suspicious. Treat as **potentially suspicious** and correlate with telemetry.

**Detection context:**

* Signature-triggered Suricata alert for a web application probe.
* Splunk analysis confirms limited, targeted probing of the ColdFusion path and no evidence of successful exploitation.
* No additional suspicious URIs, no rare/unique User-Agents, and no recent activity in the last 30 minutes.

**Impact if successful :**

* Remote Command Execution (RCE) via vulnerable CF components or misconfigured handlers.
* Data disclosure, webshell installation, persistence, lateral movement, or pivoting from a compromised web host.
* Potential privilege escalation if executed commands run with elevated rights.

**Mini Attack Visualization:**

**Suricata detects ET WEB\_SERVER ColdFusion componentutils access (Web Application Attack)]**

**↓**

**[Analyst investigates Suricata alert — source IP 145.239.154.85]**

**↓**

**[Connection observed from source port 49704 → destination 38.242.128.144:80]**

**↓**

**[HTTP GET requests targeting /CFIDE/componentutils/]**

**↓**

**[User-Agent present: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36" — likely spoofable]**

**↓**

**[Splunk correlation: 3,983 total events from IP → narrowed to 6 events for /CFIDE/componentutils/]**

**↓**

**[All 6 requests returned HTTP 404 Not Found — no successful response observed]**

**↓**

**[Threat intel: VirusTotal flags 6/95 vendors for the IP; Trustwave marks related domain as suspicious; AbuseIPDB ~960 reports]**

**↓**

**[Shodan/Censys show open services (e.g., 22, 123, 8126) — increases attack surface]**

**↓**

**[Assessment: automated ColdFusion reconnaissance/scanning; no confirmed exploitation]**

\*ACTION\*

1. **Block the Source IP (145.239.154.85)**

Block the attacker’s IP at the perimeter firewall, IDS/IPS, or WAF to prevent further reconnaissance attempts. Continue to monitor for reappearance from other IPs in the same ASN (ip-145-239-154.eu).

1. **Restrict Access to /cgi-bin/** Limit or disable public access to /CFIDE/ directories if ColdFusion is not required. If ColdFusion is in use, restrict access to admin/utility components like /CFIDE/componentutils/ to trusted IPs or internal networks only.
2. **Harden Against Path Traversal** Verify that ColdFusion is fully patched. Disable unused components and ensure error pages do not leak stack traces or version information. Confirm directory listing is disabled.

1. **Enable or Tune WAF Rules**

**Configure the Web Application Firewall to detect and block:**

* **Requests to /CFIDE/\* from untrusted sources**
* **Automated reconnaissance patterns targeting ColdFusion components**
* **Suspicious or spoofed User-Agent strings that mimic browsers but originate from mass scanners**

1. **Investigate Suspicious User-Agent (libredtail-http)  
   Review logs for other requests from IP 145.239.154.85 with the same User-Agent string**

**Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/94.0.4606.81.**

**Spoofed UA strings are common in scanning tools — correlate with request frequency and target paths.**

1. **Expand Threat Hunting via Threat Intelligence** Monitor for related activity from the domain ip-145-239-154.eu and other malicious IPs flagged in VirusTotal or AbuseIPDB. Add these indicators to watchlists for early detection.
2. **Correlate in Historical Logs**

Search Splunk/QRadar for additional requests to /CFIDE/ or other ColdFusion endpoints in the last 30–60 days. Look for any non-404 responses or POST requests that might indicate exploitation attempts.

1. **Validate QRadar SIEM Offense** The detection was initially triggered in **QRadar (Severity 9 offense)**. Verify that correlation rules are tuned to generate alerts for similar exploitation attempts.
2. **Continuous Monitoring  
   Set up alerting for future attempts targeting /CFIDE/componentutils/. Escalate if you observe successful responses (200/500), file uploads, or command execution attempts.**