Time and Date of Activity

3 September 2025 - 00:00:11.177031

An attacker from IP address 156.244.33.162 sent 272,014 requests within a 4 hour window making it the most active source observed during this time frame

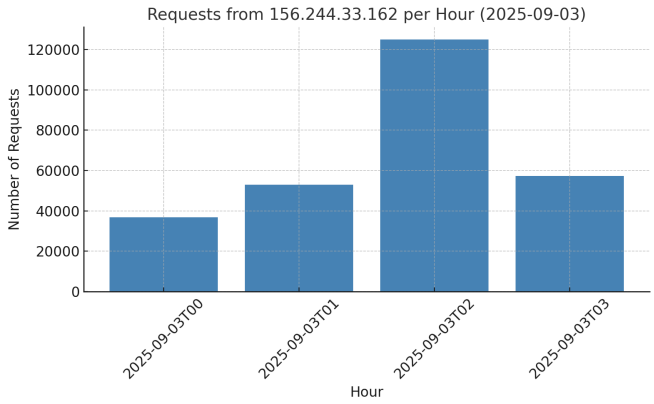
Relevant Logs, Files, or Evidence

Source: webhoneypot-2025-09-03.json

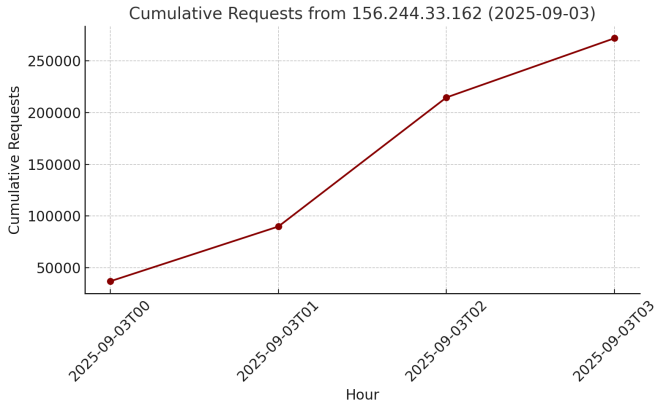
Total Requests:

```
272014 "156.244.33.162"
```

Requests per hour bar chart (UTC):



Requests per hour Cumulative Line graph(UTC):



URL extraction jq query:

```
jq -r 'select(.sip=="156.244.33.162") | .url' webhoneypot-2025-09-03.json | sort | uniq -c | sort -nr
```

Key URLs Found:
Both URLs were queried 346 times

1. /ws/msw/tenant/%27%20union%20select%20%28select%20ID%20from%20SGMSDB.DOMAINS%20limit%201%29%2C%20%27%27%2C%20%27%27%2C%20%27%27%2C%20%27%27%2C%20%27%27%2C%20%27%27%2C%20%28select%20concat%28id%2C%20%27%3A%27%2C%20password%29%20from%20sgmsdb.users%20where%20active%20%3D%20%271%27%20order%20by%20issuperadmin%20desc%20limit%201%20offset%200%29%2C%27%27%2C%20%27%27%2C%20%27
2. /%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22whoami%22%29.getInputStream%28%29%2C%22utf-8%22%29%29.%28%40com.opensymphony.webwork.ServletActionContext%40getResponse%28%29.setHeader%28%22X-Cmd-Response%22%2C%23a%29%29%7D/

Top 20 Queried URLs:

```
31167 /
13400 /wp-admin/admin-ajax.php
 5137 /index.php
 3460 /api/v1/database/6
 3460 /api/v1/database/5
 3460 /api/v1/database/4
 3460 /api/v1/database/3
 3460 /api/v1/database/10
 3460 /api/v1/database/1
 3114 /app
 3114 /api/v1/database/9
 3114 /api/v1/database/7
 2768 /api/v1/database/2
 1384 /mgmt/tm/util/bash
 1384 /cgi-bin/cstecgi.cgi
 1384 /cgi-bin/account_mgr.cgi
 1384 /CFIDE/wizards/common/utils.cfc
 1384 /ajax-api/2.0/mlflow/model-versions/create
 1374 /login
 1038 /WSVulnerabilityCore/VulCore.asmx
```

Which Vulnerability Does the Attack Attempt to Exploit?

Analysis of the requested URLs shows attempts across multiple categories:

- CVE-2023-34133 is associated with Key URL 1 and is considered a very high risk vulnerability. The attacker is attempting to exploit Improper Neutralization of Special Elements used in a SQL Command Injection vulnerability with SonicWall GMS 9.3.2-SP1 and before as well as Analytics 2.5.0.4-R7 and before

- CVE-2022-26134 is associated with Key URL 2 and is considered very high risk, attacker is attempting to exploit an unauthenticated and remote OGNL injection vulnerability to achieve code execution on a Confluence server, often associated on Linux and is internet-facing

- WordPress brute force / exploitation
    - `/wp-admin/admin-ajax.php`
    - `/xmlrpc.php`
- API fuzzing
    - `/api/v1/database/[1–10]`
- Enterprise RCE exploits
    - `/mgmt/tm/util/bash` (F5 BIG-IP CVE-2020-5902)
    - `/CFIDE/wizards/common/utils.cfc` (ColdFusion RCE)
    - `/cgi-bin/account_mgr.cgi` (legacy CGI exploit)
- Machine Learning exposure
    - `/ajax-api/2.0/mlflow/model-versions/create`

What Is the Goal of the Attack?

Attacker queried a wide range of URLs, indicative of automated mass scanning while most requests targeted common applications(WordPress, F5, ColdFusion), the main focus is on the Key URLs listed.

Attacker behavior indicates:

- Identifying and brute forcing weak WordPress Credentials
- Exploiting unpatched enterprise appliances(F5, ColdFusion)
- Attempting remote code execution via CVE-2022-26134
- If successful, these exploits lead to:
    - Remote shell access
    - Installation of malware or botnet agents
    - Hijacking compute resources for DDoS or cryptomining
    - Database Compromise

If the System is Vulnerable, Would the Attack be Successful?

Analysis of the honeypot logs indicates that multiple attempts were made to exploit both CVE-2022-26134 and CVE-2023-34133. For CVE-2022-26134, the honeypot recorded 692 HTTP 200 responses. The discrepancy on recorded status codes compared to payload attempts is explained by how the honeypot logs both initial requests and their mirrored responses as indicated in the screenshot for every attempt made by the attacker 2 logs were recorded. This can also indicate possible automated retries by the attackers tooling, leading to repeated payload attempts. However, no evidence of successful remote code execution was observed, as indicators such as returned command output or outbound DNS queries were absent.

```
2025-09-03T00:00:11.613757      156.244.33.162  200
tf-8%22%29%29.%28%40com.opensymphony.webwork.Servlet
2025-09-03T00:00:11.614466      156.244.33.162  200
2025-09-03T00:02:19.920568      156.244.33.162  200
tf-8%22%29%29.%28%40com.opensymphony.webwork.Servlet
.2025-09-03T00:02:19.921421     156.244.33.162  200
```

CVE-2023-34133, SQL injection payloads consistently returned HTTP 200 status codes, but no credential-shaped data or database error messages were present.

In conclusion, while the system demonstrated responses consistent with repeated exploitation attempts, there was no indication that the attacks achieved execution or data exfiltration. If an unpatched production system were exposed, these attempts could have succeeded, resulting in remote command execution or database compromise.

How Can the System be Protected?

CVE-2022-26134 mitigations:

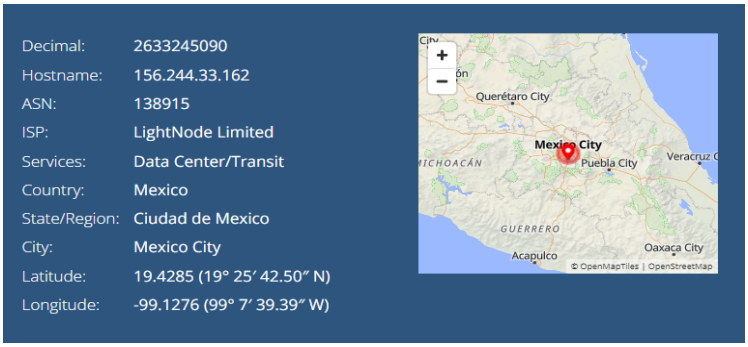
- Installing Patches
- Implement workaround if you cannot upgrade Confluence this is temporary however, it includes updating specific files depending on the version you are running as shown directly from Confluence's Support Page (https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html)
- If you cannot mitigate the vulnerability in any version of Confluence you need to restrict or disable the Confluence Server and Confluence Data Center Instances stated from rapid7
- Implement safelist IP rules
- Add WAF protection
- Java deserialization rules to defend against RCE injection

CVE-2023-34133 mitigations:

- Application isolation to limit what other processes and system features the exploited target can access
- WAF to limit exposure of applications
- All publicly facing services should be checked to ensure they should be public facing,restrict access to any that should be available only internally
- Segment externally facing servers and services from the network with a DMZ or different hosting infrastructure
- Principle of least privilege for service accounts
- Software Updates
- Scan Externally facing systems for vulnerabilities to patch systems when critical vulnerabilities are found

What Do You Know About the Attacker?

Source IP: 156.244.33.162
Geolocation: Mexico City, hosted in datacenter:



Attribution: Likely a very aggressive automated tool performing large exploitation attempts and vulnerability scanning for unpatched systems and weakly implemented authentication protection.

Behavior: Hundreds of thousands of payload/exploit attempts within a 4 hour time frame, suggesting very aggressive attempts at exploitation on web servers.

Indicators of Compromise (IOCs)

IOC for CVE-2022-26134

Type	Value
Source IP(s)	156.244.33.162
Exploit Payloads	${@java.lang.Runtime@getRuntime().exec("whoami")}, ${@java.lang.Runtime@getRuntime().exec("nslookup ...")}
Targeted Endpoint	Confluence OGNL injection via ${...} expressions
Indicators	692 HTTP 200 responses; no X-Cmd-Response or outbound DNS
External Domains	d2rc2gch7tti260lcbg...oast.live (blind RCE validation)
User-Agent(s)	Mozilla/5.0 Firefox/102.0 (likely spoofed)

IOC for CVE-2023-34133

Type	Value
Source IP(s)	156.244.33.162
Exploit Payloads	/ws/msw/tenant/' union select ... concat(id, ':', password)...
Targeted Endpoint	/ws/msw/tenant/ parameter
Attack Type	Union-based SQL Injection(Credential Extraction Attempt)
Indicators	Repeated HTTP 200s; no id:password credential strings leaked in response body
User-Agent(s)	Mozilla/5.0 Firefox/102.0 (likely spoofed)

References

CVE-2022-26134:
https://www.rapid7.com/blog/post/2022/06/02/active-exploitation-of-confluence-cve-2022-26134/

Confluence Advisory:
https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

CVE-2023-34133:
https://attackerkb.com/topics/vhcXEiZ322/cve-2023-34133?referrer=search

CVE Record: https://www.cve.org/CVERecord?id=CVE-2023-34133

MITRE ATT&CK T1190: https://attack.mitre.org/techniques/T1190/

Analyst Information

Analyst Name: Mitchell Patton
Date of Analysis: 5 September 2025