Cybersecurity Incident Report

* Report Date: May 14, 2025
* Report Prepared By: [Your Name/Team Name, e.g., IT Security Department]
* Date of Incident Discovery: May 5, 2025
* Period of Suspicious Activity: Primarily May 5, 2025, with concentrated activity from key sources between approximately 9:11 AM and 9:21 AM (System Time).
* Affected System(s): [Clearly name the web server or application, e.g., "Corporate Web Server (https://www.google.com/search?q=web01.yourdomain.com)" or "Customer Portal Application"]
* Primary External IP Address Investigated: 54.164.60.142
* Other Noteworthy External IP Addresses: 54.158.63.X (exact IP to be confirmed), 44.201.230.231

1. Overview of the Incident

Our ongoing review of web server logs (specifically, the 'fss iss logs') for May 5, 2025, brought a significant security event to light, standing out against the backdrop of routine, low-and-slow scanning activities and automated bot traffic that our web infrastructure regularly encounters. On this date, the log data, which culminated in an 'Overall Security Threat Score' of 'Critical,' indicated a more focused and concerted attack. Across 46,737 recorded entries from 1,401 unique IPs, our analysis highlighted 51 critical security events and 8,224 warnings. While many sources contributed to general scanning, intensive and hostile activity was specifically noted from the external IP address 54.164.60.142. The actions from this particular IP address went beyond passive probing, involving systematic vulnerability scanning and clear attempts to breach system security, marking it as a primary source of the direct attack.

2. Nature of the Attack and Key Observations

As highlighted in the overview, the external IP address 54.164.60.142 was particularly aggressive during a short window on May 5, 2025, specifically between 9:11:33 AM and 9:21:01 AM. During this period, this IP address alone generated 6,116 requests, operating at a high rate of approximately 646 requests per minute.

Key threatening activities observed include:

* Automated Probing and Scanning:  
  + High Request Volume: The IP 54.164.60.142 generated over 6,000 requests in a short period (approximately 646 text requests per minute), targeting 134 unique (URis) on our system. This indicates automated scanning tools were likely used.
  + Targeted URLs: Attackers focused on common login pages (/login received nearly 6,000 hits from the primary IP), as well as known administrative or vulnerable paths related to various web technologies (e.g., WordPress paths like /wp-admin/, /wp-content/plugins/, and others like /api/server/version, /mgmt/shared/authn/login).
* Attempted Exploitation Techniques:  
  + Command Injection Attempts: We observed numerous attempts to execute unauthorized system commands (e.g., id, netstat -an) by embedding them in the "User Agent" field of web requests. This is a common technique to try and gain control of a server.
  + Script and Parameter Injection: Logs show over 6,300 attempts to inject malicious scripts or parameters into our web applications.
  + Evasion Tactics: Attackers used techniques like "multiple plus signs in URLs" (over 1,500 instances) to try and disguise their malicious requests and bypass security defenses.
  + IIS Specific Exploits: 181 attempts to exploit known vulnerabilities related to Microsoft IIS error pages were recorded.
* Broader Attack Campaign:  
  + The "Attack Chain Visualization" tool suggests a multi-stage attack involving other IP addresses (54.158.63.X, 44.201.230.231). These IPs were involved in reconnaissance (scanning), exploitation attempts, gaining access, and potentially trying to establish long-term presence ("persistence"). This indicates a broader, more sophisticated attack campaign than just a single IP.

3. Identified Sources of Malicious Activity (Indicators of Compromise - IOCs)

* Key Attacking IP Addresses:
  + 54.164.60.142 (High volume of varied attacks)
  + 54.158.63.X (Linked to exploitation and persistence; full IP requires confirmation)
  + 44.201.230.231 (Involved in reconnaissance and access attempts)
* Suspicious User-Agent Strings (Examples of attempted commands):
  + netstat -an
  + id
  + ;id
  + /usr/bin/id
* Targeted URLs Indicating Specific Vulnerability Probes:
  + /login (Brute-force/credential stuffing)
  + WordPress-related paths (e.g., /wp-admin/, /wp-content/plugins/)
  + /NmAPI/RecurringReport (High-risk target)
  + /global-protect/portal/images/?wlcu089gxCxGgD3pi3EFh77Emz.txt (Suspicious file access)

4. Assessed Risk and Potential Business Impact

* Severity Level: CRITICAL
* Potential Impact: If these attacks were successful, the consequences could include:
  + Unauthorized access to sensitive data or customer data.
  + Full system compromise, allowing attackers to control the server.
  + Service disruption or website defacement.
  + Use of our systems to launch attacks against other targets.
  + Damage to our organization's reputation.

5. Current Status and Actions Taken

* Initial log analysis and incident assessment completed.

6. Recommended Next Steps and Mitigation Strategies

To address this incident and strengthen our defenses, we recommend the following actions:

* Immediate Actions:  
  1. Block Malicious IPs: Ensure all identified attacking IP addresses (54.164.60.142, 54.158.63.X, 44.201.230.231) are blocked at the network firewall or Web Application Firewall (WAF).
  2. Deep Dive Investigation: Conduct a thorough investigation into the activities of IPs 54.158.63.X and 44.201.230.231, focusing on signs of successful exploitation or persistence.
  3. Vulnerability Assessment: Scan the affected systems for vulnerabilities exploited by these attack types (e.g., outdated software, IIS misconfigurations, injection vulnerabilities).
  4. Security Log Review: Examine server and application logs in detail for any signs of successful compromise, beyond the initial alerts.
  5. Secure Login Mechanisms: Review and enhance security for all login pages. Implement strong password policies, account lockout mechanisms after failed attempts, and Multi-Factor Authentication (MFA) where feasible.
* System Hardening & Preventative Measures:  
  1. Patch Management: Ensure all server software, web applications (including WordPress and its plugins, if applicable), and security devices are updated with the latest security patches.
  2. Web Application Firewall (WAF) Tuning: Review and enhance WAF rules to specifically block command injection, script injection, and common evasion techniques.
  3. Input Validation: Enforce strict input validation on all user-supplied data in web applications.
  4. Principle of Least Privilege: Ensure web server processes and application accounts have only the minimum necessary permissions.
  5. Regular Security Audits: Schedule regular security audits and penetration tests to proactively identify and address vulnerabilities.

7. Conclusion

The suspicious activity detected on May 5, 2025, represents a serious attempt to compromise our web systems. While initial analysis points to aggressive automated attacks, further investigation is crucial, especially concerning the IPs flagged in the "Attack Chain Visualization" for potential deeper compromise. Prompt action on the recommended steps will be vital to mitigate the current threat and improve our overall security posture.