BREAKING CYBERSECURITY NEWS: TWO DISTINCT BOTNETS EXPLOIT WAZUH SERVER VULNERABILITY TO LAUNCH MIRAI-BASED ATTACKS

Vairav Cyber Security News Report

Date: June 10, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical remote code execution vulnerability (CVE-2025-24016) in Wazuh Server, an open-source SIEM and security monitoring platform, has been actively exploited by Mirai-based IoT botnets to deploy DDoS malware. This poses serious risks to organizations relying on Wazuh for security oversight.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The vulnerability, CVE-2025-24016, arises from unsafe deserialization in Wazuh's DistributedAPI, where JSON serialized data is processed using as_wazuh_object, leading to remote code execution. Mirai botnet operators have weaponized this flaw: two distinct variants were observed one was active since early March, fetching shell scripts to deploy Mirai, and another since May using Italian-named domains targeting Italian-speaking devices. This vulnerability affects Wazuh Server version 4.4.0 prior to version 4.9.1.

Identification: The vulnerability was identified by Wazuh on February 10, 2025, and patched with release 4.9.1. The public release of exploit code was released on March, 2025. Researchers at Akamai confirmed active exploitation via Mirai beginning in March and again in May.

Affected Entities/Industries:

- Organizations deploying wazuh-manager versions 4.4.0 to 4.9.0 are at risk.
- IoT device ecosystems (e.g., routers, cameras) also targeted indirectly via Mirai-infected Wazuh servers.

Potential Impact:

- Successful exploitation enables arbitrary code execution: attackers can control or shutdown Wazuh servers, disrupt monitoring, and facilitate lateral movement.
- Infected servers become part of Mirai botnets, used for DDoS attacks and further IoT infection.

- Impacts include data integrity compromise, security infrastructure downtime, and elevated risk posture.

Exploitation Methods:

- Attackers must first obtain API credentials (e.g. via stolen dashboard login).
- Craft malicious JSON with the __unhandled_exc__ key to trigger deserialization exploit, often via the run_as API or compromised agents.
- Payloads target both master and worker servers within Wazuh clusters, and compromised agents may relay malicious configurations

RELATED THREAT INTELLIGENCE & IOCs

Malicious IPs

- 209.141.34[.]106
- 176.65.142[.]137
- 65.222.202[.]53
- 196.251.86[.]49
- 176.65.134[.]62
- 104.168.101[.]27
- 104.168.101[.]23
- 79.124.40[.]46
- 194.195.90[.]179

Suspicious Domains

- nuklearcnc.duckdns[.]org
- jimmyudp-raw[.]xyz
- pangacnc[.]com
- neon.galaxias[.]cc
- cbot.galaxias[.]cc
- resbot[.]online
- versioneonline[.]com

- web-app-on[.]com
- Assicurati-con-linear[.]online
- webdiskwebdisk.webprocediweb[.]com
- continueoraweb[.]com
- ora-0-web[.]com
- adesso-online[.]com
- multi-canale[.]com
- eversioneweb[.]com
- gestisciweb[.]com

Malware Hashes (SHA256)

- dece5eaeb26d0ca7cea015448a809ab687e96c6182e56746da9ae4a2b16edaa9
- 7b659210c509058bd5649881f18b21b645acb42f56384cbd6dcb8d16e5aa0549
- 64bd7003f58ac501c7c97f24778a0b8f412481776ab4e6d0e4eb692b08f52b0f
- 4c1e54067911aeb5aa8d1b747f35fdcdfdf4837cad60331e58a7bbb849ca9eed
- 811cd6ebeb9e2b7438ad9d7c382db13c1c04b7d520495261093af51797f5d4cc
- 90df78db1fb5aea6e21c3daca79cc690900ef8a779de61d5b3c0db030f4b4353
- 8a58fa790fc3054c5a13f1e4e1fcb0e1167dbfb5e889b7c543d3cdd9495e9ad6
- c9df0a2f377ffab37ede8f2b12a776a7ae40fa8a6b4724d5c1898e8e865cfea1
- 6614545eec64c207a6cc981fccae8077eac33a79f286fc9a92582f78e2ae243a
- 9d5c10c7d0d5e2ce8bb7f1d4526439ce59108b2c631dd9e78df4e096e612837b
- be4070b79a2f956e686469b37a8db1e7e090b9061d3dce73e3733db2dbe004f0
- e6cf946bd5a17909ae3ed9b1362cfaafa7afe02e74699dcbc3d515a6f964b0b0
- 4d9f632e977b16466b72b6ee90b6de768c720148c1e337709b57ca49c1cdffb6
- a0b47c781e70877ad4e721ba49f64fc0bc469e38750f070a232d12f03d9990bc
- 941a30698db98f29919cba80e66717c25592697b1447f3e96825730229d97549

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Upgrade to wazuh-manager 4.9.1+ which patches the insecure JSON deserialization flaw.
- Restrict API access allowing only trusted networks and credentials for API endpoints.
- Monitor logs and flag unusual API calls (e.g., run_as, getconfig) or unfamiliar JSON structures.

Security Best Practices

- Enforce strong authentication, preferably MFA, for all API users.
- Harden agent configurations to prevent third-party agents from exploiting master/worker communication.
- Regularly analyze incoming/outgoing network traffic for signs of botnet communication.

For Advanced Security Teams

- Deploy intrusion detection focusing on signature-based detection for Mirai payload download activity.
- Utilize threat intel feeds to block the known malicious IP and domain IOCs.
- Conduct penetration tests simulating run_as endpoint misuse to validate defenses.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/06/botnet-wazuh-server-vulnerability.html
- https://www.akamai.com/blog/security-research/botnets-flaw-mirai-spreads-through-wazuh-vulnerability#iocs
- https://app.opencve.io/cve/CVE-2025-24016

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com