Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

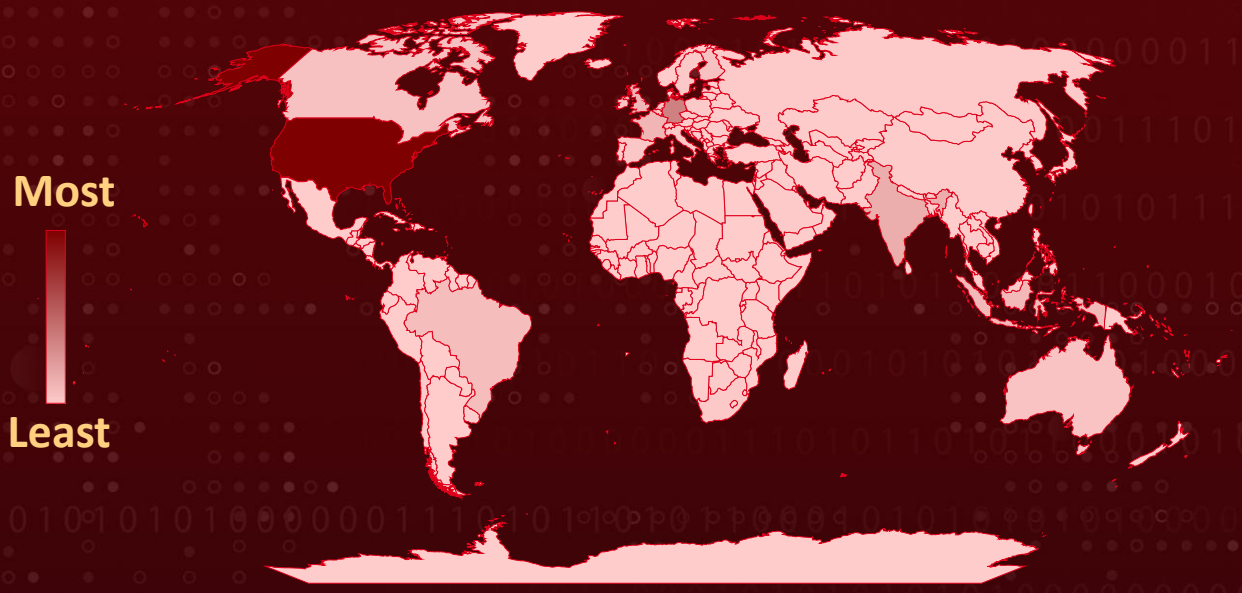
Wazuh Server Vulnerability Hijacked by Mirai Variants

Date of Publication	Admiralty Code	TA Number
June 13, 2025	A1	TA2025187

Summary

Attack Commenced: March 2025
Botnet: Mirai, Resbot (aka Resentual)
Targeted Region: Worldwide
Attack: In late March 2025, a critical Wazuh vulnerability CVE-2025-24016 has fallen into active exploitation, with cybercriminals leveraging it to unleash multiple Mirai botnet variants. This rapid weaponization highlights a stark reality of today's threat landscape: the window between vulnerability disclosure and widespread exploitation is collapsing at an alarming pace. For defenders, it's a sobering reminder that no vulnerability remains idle for long and adversaries are faster, sharper, and more opportunistic than ever.

Targeted Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-24016	Wazuh Server Deserialization of Untrusted Data Vulnerability	Wazuh Server version 4.4.0 to 4.9.0	✗	✓	✓

Attack Details

#1 In late March 2025, cybercriminals began exploiting a critical vulnerability in Wazuh, an open-source XDR and SIEM platform widely used by over 100,000 organizations globally, including numerous Fortune 100 companies. The flaw, tracked as CVE-2025-24016, is an unsafe deserialization vulnerability that enables remote code execution through the Wazuh API.

#2 At the core of the issue lies the DistributedAPI, where parameters are serialized as JSON and deserialized using the as_wazuh_object method in the framework/wazuh/core/cluster/common.py file. Threat actors can exploit this by injecting malicious JSON payloads to execute arbitrary Python code on targeted systems. Not long after its proof-of-concept (**PoC**) disclosure, exploitation attempts surfaced, linking the vulnerability to two distinct botnet campaigns.

#3 The first emerged in early March 2025, when attackers deployed a malicious shell script that downloaded and executed a Mirai malware variant known as "morte." This particular strain belongs to the LZRD Mirai family, easily identified by the hardcoded string “lzrd here” displayed on infected systems.

#4 By early May 2025, a second botnet operation began exploiting the same Wazuh vulnerability. This campaign used a similar delivery method, a malicious shell script to install another Mirai-based variant dubbed Resbot, also known as Resentual.

#5 These incidents highlight an ongoing and concerning trend. Botnet operators are rapidly narrowing the window between vulnerability disclosure and active exploitation. By closely monitoring newly published CVEs and swiftly repurposing public PoC code, these actors can quickly expand existing botnets or establish new ones.

Recommendations

Eliminate Exploitation Conditions for CVE-2025-24016: To mitigate the risk of CVE-2025-24016 exploitation, organizations should immediately upgrade any Wazuh deployments running versions 4.4.0 to 4.9.0, strictly avoid exposing the Wazuh API to the internet, and enforce strong credential hygiene by replacing default administrator credentials, applying complex password policies, and regularly auditing API access. These simple, proactive actions eliminate the core conditions that make exploitation possible.

Monitor Malicious Payload Delivery Paths: Monitor and restrict outbound connections from your servers to untrusted external sources. Mirai-based botnets typically download payloads via malicious shell scripts; blocking these outbound calls at the firewall or proxy layer can break the infection chain.

Maintain an Accurate Asset and Version Inventory: Keep a real-time, centralized inventory of all deployed software versions, particularly for critical infrastructure like SIEM, XDR, firewalls, and VPN appliances. This allows for immediate identification of vulnerable systems upon CVE disclosures.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0011** Command and Control	**TA0042** Resource Development	**T1584.005** Botnet
T1190 Exploit Public-Facing Application	**T1078** Valid Accounts	**T1059** Command and Scripting Interpreter	**T1071.001** Web Protocols
T1071 Application Layer Protocol	**T1105** Ingress Tool Transfer	**T1543** Create or Modify System Process	**T1018** Remote System Discovery
T1046 Network Service Discovery	**T1562** Impair Defenses	**T1027** Obfuscated Files or Information	**T1496** Resource Hijacking
T1584 Compromise Infrastructure	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1078.001** Default Accounts

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	209[.]141[.]34[.]106, 176[.]65[.]142[.]137, 65[.]222[.]202[.]53,

TYPE	VALUE
IPv4	196[.]251[.]86[.]49, 176[.]65[.]134[.]62, 104[.]168[.]101[.]27, 104[.]168[.]101[.]23, 79[.]124[.]40[.]46, 194[.]195[.]90[.]179
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
SHA256	dece5eaeb26d0ca7cea015448a809ab687e96c6182e56746da9ae4a2b16edaa9, 7b659210c509058bd5649881f18b21b645acb42f56384cbd6dcb8d16e5aa0549, 64bd7003f58ac501c7c97f24778a0b8f412481776ab4e6d0e4eb692b08f52b0f, 4c1e54067911aeb5aa8d1b747f35fdcdfdf4837cad60331e58a7bbb849ca9eed, 811cd6ebeb9e2b7438ad9d7c382db13c1c04b7d520495261093af51797f5d4cc, 90df78db1fb5aea6e21c3daca79cc690900ef8a779de61d5b3c0db030f4b4353, 8a58fa790fc3054c5a13f1e4e1fcb0e1167dbfb5e889b7c543d3cdd9495e9ad6, c9df0a2f377ffab37ede8f2b12a776a7ae40fa8a6b4724d5c1898e8e865cfea1, 6614545eec64c207a6cc981fccae8077eac33a79f286fc9a92582f78e2ae243a, 9d5c10c7d0d5e2ce8bb7f1d4526439ce59108b2c631dd9e78df4e096e612837b, be4070b79a2f956e686469b37a8db1e7e090b9061d3dce73e3733db2dbe004f0,

TYPE	VALUE
SHA256	e6cf946bd5a17909ae3ed9b1362cfaafa7afe02e74699dcbc3d515a6f964b0b0, 4d9f632e977b16466b72b6ee90b6de768c720148c1e337709b57ca49c1cdffb6, a0b47c781e70877ad4e721ba49f64fc0bc469e38750f070a232d12f03d9990bc, 941a30698db98f29919cba80e66717c25592697b1447f3e96825730229d97549

Patch Links

https://github.com/wazuh/wazuh/releases/tag/v4.9.1

https://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh

References

https://www.akamai.com/blog/security-research/botnets-flaw-mirai-spreads-through-wazuh-vulnerability

https://wazuh.com/blog/addressing-the-cve-2025-24016-vulnerability/

https://github.com/MuhammadWaseem29/CVE-2025-24016

https://hivepro.com/threat-advisory/mirai-botnet-exploits-multiple-flaws-in-the-latest-campaign/

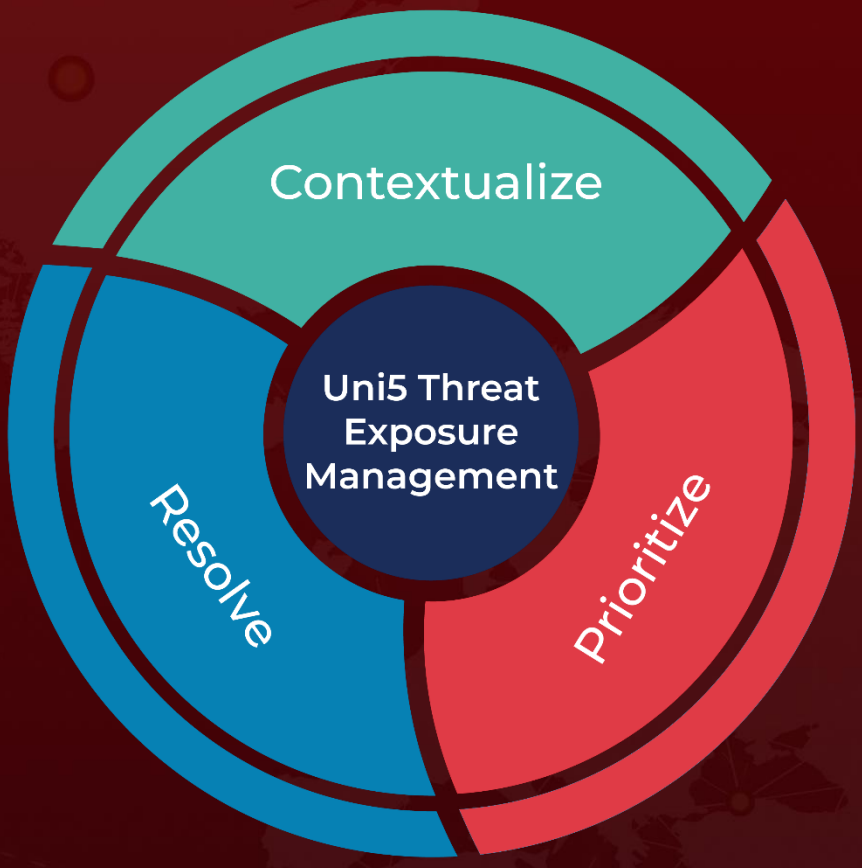
https://hivepro.com/threat-advisory/deciphering-mirais-next-chapter-the-strategies-of-the-latest-players/

https://hivepro.com/threat-advisory/growing-threat-of-earth-estries-group-behind-major-telecom-breaches-2/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 13, 2025 • 6:00 AM

More at www.hivepro.com