An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2503140157

NCSC Advisory

Wazuh Server RCE Vulnerability
CVE-2025-24016

14th, March 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-24016

Published: 2025-02-10

Vendor: Wazuh

Product: Wazuh Server

CVSS Score[1]: 9.9

Products Affected

Product	Version
Wazuh server	>= 4.4.0 < 4.9.1

Impact

This is a remote code execution (RCE) vulnerability in Wazuh server, introduced by an unsafe deserialization in the wazuh-manager package. The vulnerability allows remote attackers with API access (compromised dashboard, Wazuh servers in the cluster, or certain configurations with compromised agents) to execute arbitrary code on the server.

Common Weakness Enumeration (CWE)[2]: CWE-502: Deserialization of Untrusted Data

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

Upgrading to Wazuh 4.9.1 or later is the best way to address this issue since it includes the patch that addresses the vulnerability. In addition, limiting API access to only essential and trusted clients can help minimize risks.

NCSC strongly recommends installing updates for vulnerable systems with the highest priority and after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Wazuh.

- https://nvd.nist.gov/vuln/detail/CVE-2025-24016
- https://www.cve.org/CVERecord?id=CVE-2025-24016
- https://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh
- https://www.sonicwall.com/blog/critical-wazuh-rce-vulnerability-cve-2025-24016-risks-exploits-and-remediation