An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605130242

NCSC Advisory

Critical Path Traversal Vulnerability in Wazuh

CVE-2026-30893

13th, May 2026

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-2026-30893

Published: 2026-04-29

Vendor: Wazuh

Product: Wazuh XDR & SIEM

CVSS Score[1]: 9.0

Products Affected

Product	Version
wazuh	>= 4.4.0, < 4.14.4

Impact

Wazuh is a free and open source platform used for threat prevention, detection, and response. From version 4.4.0 to before version 4.14.4, a path traversal vulnerability in Wazuh's cluster synchronization extraction routine allows an authenticated cluster peer to write arbitrary files outside the intended extraction directory on other cluster nodes.

This can be escalated to code execution in the Wazuh service context by overwriting Python modules loaded by Wazuh components (proof of concept available as separate attachment). In deployments where the cluster daemon runs with elevated privileges, system-level compromise is possible. This issue has been patched in version 4.14.4.

Common Weakness Enumeration (CWE)[2]:

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
- CWE-73: External Control of File Name or Path

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

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, 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-2026-30893
- https://www.cve.org/CVERecord?id=CVE-2026-30893
- https://github.com/wazuh/wazuh/security/advisories/GHSA-m8rw-v4f6-8787
- https://github.com/wazuh/wazuh/releases/tag/v4.14.4