مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Wazuh Manager Inventory Sync

Tracking #:432319137

Date:15-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the inventory synchronization subsystem of Wazuh Manager version 5.0.0-beta1.

TECHNICAL DETAILS:

A critical vulnerability has been identified in the inventory synchronization subsystem of Wazuh Manager version 5.0.0-beta1. The flaw allows an attacker to inject arbitrary OpenSearch _bulk operations through an unsanitized agent-controlled field (DataValue.index), resulting in unauthorized document manipulation within the Wazuh Indexer.
The vulnerability carries a maximum CVSS v3.1 score of 10.0 (Critical) and can be exploited remotely by an attacker who enrolls a rogue agent. Successful exploitation enables arbitrary deletion, modification, and creation of OpenSearch documents, potentially allowing attackers to tamper with alerts, erase forensic evidence, modify vulnerability data, and compromise analyst dashboards.

Vulnerability Details:

- GHSA ID: GHSA-ff9g-85jq-r3g3
- CVE: No CVE assigned
- Severity: Critical
- CVSS Score: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- Affected Component: inventory_sync and indexer_connector
- Affected Product: Wazuh Manager
- Affected Version: >= 5.0.0-beta1
- Fixed Version: 5.0.0-beta3
- Weaknesses: CWE-74, CWE-93, CWE-863

RECOMMENDATIONS:

Immediate Actions:

- Upgrade Wazuh Manager to fixed version or later immediately.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/wazuh/wazuh/security/advisories/GHSA-ff9g-85jq-r3g3