مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in Elastic Fleet Server

Tracking #:432316792

Date:27-01-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Elastic Fleet Server, which could be exploited to gain unauthorized access to sensitive data on affected systems.

## TECHNICAL DETAILS:

**Vulnerability Details:**

- **CVE-2024-52975**
- CVSS Score: 9.0 (Critical)
- Critical Vulnerability exists in Elastic Fleet Server where Fleet policies containing sensitive information were logged on INFO and ERROR log levels. The nature of the sensitive information largely depends on the integrations enabled. This vulnerability could allow unauthorized individuals to access sensitive data, potentially leading to data breaches and other security risks
- Exploitation of this vulnerability could result in:
    - Unauthorized access to sensitive information within Fleet logs.
    - Potential data breaches and compromised security of Elastic Agent deployments.

**Affected Versions**

- Fleet Server versions from 8.13.0 up to 8.15.0

**Fixed Version:**

- Fleet Server 8.15.0 or later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://nvd.nist.gov/vuln/detail/CVE-2024-52975