مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Elastic Cloud Enterprise (ECE)

Tracking #:432317812

Date:14-10-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Elastic has released security updates for Elastic Cloud Enterprise (ECE) to address a critical template injection vulnerability in the Jinjava engine that can lead to server-side code execution and data exfiltration.

TECHNICAL DETAILS:

Elastic has released urgent security updates to address a critical vulnerability in Elastic Cloud Enterprise (ECE) that could allow attackers with administrative access to exfiltrate sensitive information or execute arbitrary commands through template injection in the Jinjava engine.

Vulnerability Details

- **CVE-2025-37729**
- Severity: Critical
- CVSS Score: 9.1
- Impact: Allows authenticated attackers with administrative privileges to inject malicious templates that execute arbitrary commands or extract sensitive information via Jinjava variable evaluation.
- Cause: Improper neutralization of special characters in user-supplied strings processed by Jinjava.
- Attack Vector: Admin console access to deployments with Logging+Metrics enabled. Malicious payloads can be injected and results read back from ingested logs.

Affected Versions:

- Versions from 2.5.0 up to and including 3.8.1
- Versions from 4.0.0 up to and including 4.0.1

Fixed Versions:

- Elastic Cloud Enterprise 3.8.2
- Elastic Cloud Enterprise 4.0.2

Indicators of Compromise (IOC)

Monitor the request logs for malicious payloads, by using the search query:

- (payload.name : int3rpr3t3r or payload.name : forPath)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Elastic.

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://discuss.elastic.co/t/elastic-cloud-enterprise-ece-3-8-2-and-4-0-2-security-update-esa-2025-21/382641