مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in Elastic Cloud Enterprise (ECE)

Tracking #:432317918

Date:03-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Elastic has released security updates addressing a high-severity Improper Authorization vulnerability in Elastic Cloud Enterprise (ECE).

TECHNICAL DETAILS:

Elastic has released security updates addressing a high-severity Improper Authorization vulnerability in Elastic Cloud Enterprise (ECE).The flaw (CVE-2025-37736) allows a built-in read only user to perform privileged API operations that should normally be restricted to administrative accounts.

Exploitation of this vulnerability could allow unauthorized privilege escalation, enabling attackers or compromised readonly accounts to create, modify, or delete users and service accounts. Given the potential for unauthorized access control manipulation, this issue poses a serious risk to multi-tenant Elastic deployments and internal infrastructure integrity.

Vulnerability Details

- CVE ID: CVE-2025-37736
- Severity Score: 8.8 (High)
- Impact: Privilege Escalation, Unauthorized API Access
- **Affected Versions:**
  - ECE 3.8.1 – 3.8.2
  - ECE 4.0.1 – 4.0.2
- **Fixed Versions**:
  - ECE 3.8.3 / 4.0.3 or later
- **For Users that Cannot Upgrade:**
  - Users that cannot upgrade, should also use the provided tooling by Elastic to list users or service accounts that have been created by the readonly user and potentially delete them.

RECOMMENDATIONS:

- Upgrade Elastic Cloud Enterprise to fixed version.
- Review all existing users and service accounts.
- Identify and remove any users or API keys created by the readonly user.

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-3-8-3-and-4-0-3-security-update-esa-2025-22/383132