مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Elastic Defend

Tracking #:432317980

Date:10-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Elastic has released security updates to address a high-severity vulnerability in Elastic Defend, the endpoint protection component of the Elastic Security suite. The flaw could allow local attackers to delete arbitrary files with SYSTEM-level privileges, potentially leading to local privilege escalation.

TECHNICAL DETAILS:

Vulnerability Details

- CVE-2025-37735
- **Severity:** High (CVSS 7.0)
- An Improper Preservation of Permissions issue in Elastic Defend for Windows may allow a local attacker to exploit the high-privilege Defend service to delete arbitrary files on the system.
  Successful exploitation could result in privilege escalation to SYSTEM, enabling full control over the affected host.
- **Affected Versions:** Elastic Defend Versions up to and including 8.19.5, and versions from 9.0.0 up to and including 9.1.5.

Impact

Successful exploitation could allow a **local attacker** to delete protected system files and **gain SYSTEM privileges**, potentially leading to full system compromise.

Fixed Versions

- 8.19.6
- 9.1.6
- 9.2.0

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-defend-8-19-6-9-1-6-and-9-2-0-security-update-esa-2025-23/383272