مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Cisco ClamAV

Tracking #:432317394

Date:19-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco disclosed two security vulnerabilities in the ClamAV engine—used widely for malware scanning across email systems, gateways, storage servers, and endpoint protection suites.

TECHNICAL DETAILS:

Cisco disclosed two security vulnerabilities in the ClamAV engine—used widely for malware scanning across email systems, gateways, storage servers, and endpoint protection suites.

Vulnerability Details:

- CVE-2025-20260 is rated **CVSS 9.8 (Critical)** and involves a heap-based buffer-overflow in the PDF scanning component. Under certain configurations, this can trigger DoS or remote code execution (RCE)
- CVE-2025-20234 (CVSS 5.3, Medium) concerns a memory over-read in UDF file scanning, leading to Denial of Service

Affected Versions:

- ClamAV < 1.4.3
- Long-Term Support: < 1.0.9
- PDF issue first exploitable from 1.0.0 onward; UDF issue from 1.2.0 onward

Fixed Versions:

- All users: Upgrade to ClamAV 1.4.3
- LTS users: Upgrade to ClamAV 1.0.9

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to immediately update the affected versions to the fixed or latest versions released by ClamAV.

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://blog.clamav.net/2025/06/clamav-143-and-109-security-patch.html