مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Command Injection Vulnerability in Libraesva ESG

Tracking #:432317743

Date:23-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical command injection vulnerability (CVE-2025-59689) has been identified in Libraesva ESG, an enterprise-grade email security gateway.

TECHNICAL DETAILS:

A critical command injection vulnerability (CVE-2025-59689) has been identified in Libraesva ESG, an enterprise-grade email security gateway. The flaw arises from improper sanitization during the removal of active code within compressed email attachments. Attackers can exploit the vulnerability by sending a specially crafted compressed archive via email, leading to arbitrary command execution under a non-privileged account.
Libraesva has released emergency patches for all supported versions (5.0–5.5) and applied them automatically to cloud and on-premise ESG appliances. However, legacy 4.x versions remain unprotected and require manual upgrade to 5.x.
One confirmed incident of active exploitation has been reported, attributed to a foreign state-sponsored threat actor, highlighting the urgency of remediation.

Vulnerability Details

- CVE ID: CVE-2025-59689
- Affected Product: Libraesva ESG v4.5+
- Attack Vector: Malicious email containing specially crafted compressed archives
- Impact: Arbitrary command execution as non-privileged user
- Exploitation: Confirmed

Affected and Fixed Versions:

- ESG 5.0 → 5.0.31
- ESG 5.1 → 5.1.20
- ESG 5.2 → 5.2.31
- ESG 5.3 → 5.3.16
- ESG 5.4 → 5.4.8
- ESG 5.5 → 5.5.7
- Versions below 5.0 are End-of-Support (EOS). Immediate manual upgrade to 5.x is required.
- Libraesva cloud customers- All appliances in Libraesva cloud have been upgraded to the latest version containing the fix. No further action needed.

RECOMMENDATIONS:

- **Immediate Upgrade:** Ensure ESG systems are running the fixed versions.

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.

REFERNCES:

- https://docs.libraesva.com/knowledgebase/security-advisory-command-injection-vulnerability-cve-2025-59689/