مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Lantronix

Tracking #:432319186

Date:24-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been disclosed in Lantronix EDS5000 that is being actively exploited in the wild.

TECHNICAL DETAILS:

A critical vulnerability, CVE-2025-67038 (CVSS v3.1: 9.8), has been disclosed in Lantronix EDS5000 version 2.1.0.0R3. The vulnerability is reported to be actively exploited in the wild and allows unauthenticated attackers to execute arbitrary operating system commands with root privileges.

Vulnerability Details

- CVE ID: CVE-2025-67038
- Severity: Critical
- CVSS v3.1 Score: 9.8 (Critical)
- The HTTP RPC module executes a shell command when logging failed authentication attempts. The supplied username parameter is directly concatenated into the shell command without proper sanitization or input validation.
- An attacker can inject arbitrary operating system commands through the username parameter. These injected commands are executed with root privileges, allowing complete control over the affected device.
- Affected Product: Lantronix EDS5000
- Affected Version: 2.1.0.0R3
- Attack Vector: Network
- Authentication Required: None
- User Interaction: None
- Impact: Remote Code Execution with root privileges

RECOMMENDATIONS:

Immediate Actions:

- Identify all affected Lantronix EDS5000 devices within the environment.
- Upgrade to a vendor-fixed firmware release as soon as it becomes available**.**

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://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657/Latest+Firmware+for+the+EDS5000+series+EDS5008+EDS5016+EDS5032.