

CVE-2025-67038

Lantronix EDS5000 Code Injection Vulnerability

CISA KEV since Jun 23, 2026

Actively exploited

An issue was discovered in Lantronix EDS5000 2.1.0.0R3. The HTTP RPC module executes a shell command to write logs when user's authentication fails. The username is directly concatenated with the command without any sanitization. This allow attackers to inject arbitrary OS commands into the username parameter. Injected commands are executed with root privileges.

EVRS 75 _{/100} Urgent priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.200 97.4th percentile · FIRST	CISA DEADLINE Jun 26, 2026 CISA federal deadline · Overdue by 4 months
--	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.200 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions · 58 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
eds5008 firmware	< 2.2.0.0r1	2.2.0.0r1	NVD
eds5016 firmware	< 2.2.0.0r1	2.2.0.0r1	NVD
eds5032 firmware	< 2.2.0.0r1	2.2.0.0r1	NVD
g526gp12s firmware	< 2.6.0.4R6	2.6.0.4R6	NVD
g526gp17s firmware	< 2.6.0.4R6	2.6.0.4R6	NVD
g526gp1cs firmware	< 2.6.0.4R6	2.6.0.4R6	NVD
g526gp1asg firmware	< 2.6.0.4R6	no fixed version listed	NVD
g526gp1as firmware	< 2.6.0.4R6	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-55gq-23mv-cw8r	ltrxdev.atlassian.net	ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657/Latest+Firmware+for+the+EDS5000+series+EDS5008+EDS5016+EDS5032
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2025-67038	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-208587	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-67038

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.