INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 18:38 UTC

BRIDGE:BREAK: 22 Vulnerabilities in Lantronix and Silex Serial-to-IP Converters Enable ICS Device Takeover

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0063
Type	CVE Vulnerability
CVE ID	CVE-2026-32955, CVE-2026-32956, CVE-2026-32961, CVE-2025-67041, CVE-2025-67034, CVE-2025-67035, CVE-2025-67036, CVE-2025-67037, CVE-2025-67038, CVE-2026-32963, CVE-2015-5621, CVE-2024-24487, CVE-2026-32960, CVE-2025-67039, CVE-2026-32965, CVE-2025-70082, CVE-2026-32958, CVE-2026-32962, CVE-2026-32964, CVE-2026-32959, CVE-2026-32957
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0004 (12th percentile)
Affected Products	Lantronix EDS3000PS Series, Lantronix EDS5000 Series, Silex SD330-AC serial-to-IP converters
Published	2026-04-21T11:46:00
Discovery Source	Rss

Executive Summary

Forescout Research Vedere Labs disclosed 22 vulnerabilities, collectively named BRIDGE:BREAK, in Lantronix EDS3000PS, EDS5000, and Silex SD330-AC serial-to-IP converters, devices that connect legacy industrial equipment to IP networks. An unauthenticated remote attacker can exploit these flaws to execute arbitrary code, bypass authentication, tamper with firmware, and achieve full device takeover. The vulnerability set includes a legacy 2015 SNMP flaw (CVE-2015-5621) still present in current firmware, highlighting the persistence of unpatched components in these devices. Organizations running these converters in operational technology environments face loss of control over physical processes and connected industrial systems.

Technical Analysis

Forescout Research Vedere Labs identified 22 CVEs across three serial-to-IP converter product lines: Lantronix EDS3000PS Series, Lantronix EDS5000 Series, and Silex SD330-AC. Vulnerability classes span OS command

injection (CWE-78), authentication bypass (CWE-287, CWE-306), unrestricted file upload enabling firmware tampering (CWE-434), resource exhaustion (CWE-400), and information disclosure (CWE-200). CVE-2015-5621, a legacy SNMP vulnerability from 2015, is included in the disclosure, indicating at least one long-unpatched component persists in affected firmware. MITRE ATT&CK coverage includes T1190 (exploit public-facing application), T1542 (pre-OS boot/firmware manipulation), T0831 (manipulation of control), T1059 (command execution), T1565 (data manipulation), and T1040 (network sniffing), among others. Approximately 20,000 devices are estimated to be exposed on the public internet. The attack vector is network-accessible; exploitation requires no authentication for the most critical flaws. Both Lantronix and Silex have issued patches. EPSS score is 0.04% (12th percentile); no CISA KEV listing at time of this report. CVSS base score: 7.5.

Action Checklist

1. Step 1: Containment. Immediately identify all Lantronix EDS3000PS, EDS5000, and Silex SD330-AC devices in your environment. Isolate internet-facing instances by removing direct public internet access; place them behind a firewall or OT DMZ. If isolation is not immediately possible, block inbound access on management ports (typically TCP 80, 443, 23, 161/UDP) at the perimeter.
2. Step 2: Detection. Query your asset inventory and network discovery tools for Lantronix EDS and Silex SD330-AC devices. Run internal network scans to identify all instances; use Shodan queries for 'Lantronix EDS' or 'Silex SD330' to verify that external exposure exists (note: Shodan results identify publicly indexed instances only and are supplementary to internal discovery). Review firewall and NGFW logs for unexpected inbound connections to serial-to-IP converter management interfaces. Check SIEM for SNMP traffic anomalies referencing CVE-2015-5621-era MIB OIDs. No public IOC patterns (hashes, IPs) are confirmed at this time.
3. Step 3: Eradication. Apply vendor-issued patches from Lantronix (for EDS3000PS and EDS5000 series) and Silex (for SD330-AC). Contact vendor support directly for patched firmware images; patches are confirmed available as of 2026-03-04. Verify firmware integrity against vendor-provided checksums before deployment. Disable SNMP v1/v2 where not required; if SNMP is required, upgrade to SNMPv3 with authentication.
4. Step 4: Recovery. After patching, confirm firmware version matches vendor-specified patched release for each device. Re-enable managed network access only after patch verification. Monitor affected devices for anomalous command execution, unexpected file uploads, or unauthorized configuration changes for a minimum of 30 days post-remediation. Validate that serial-connected ICS devices are operating within expected parameters.
5. Step 5: Post-Incident. This disclosure highlights persistent risks from legacy serial-to-IP bridging devices in OT environments: (1) CVE-2015-5621's presence confirms these devices often carry unpatched components for years; implement a formal OT asset lifecycle and patch tracking process; (2) ~20,000 internet-exposed instances indicate insufficient network segmentation is widespread; enforce OT/IT network segmentation with explicit deny-all defaults for serial converter management interfaces; (3) Map control gaps against NIST SP 800-82 (OT security) and ICS-specific MITRE ATT&CK for ICS techniques T0831, T0836, and T0859.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and OT operations leadership immediately if any Lantronix EDS or Silex SD330-AC device is confirmed internet-exposed without compensating firewall controls, if syslog or network logs show active inbound connections to management ports from external IPs prior to containment, or if serial-connected ICS devices show unexpected parameter changes that could indicate pre-patch compromise enabling MITRE ATT&CK for ICS T0831 or T0836.
Recovery Notes	After applying vendor-patched firmware to each Lantronix EDS3000PS, EDS5000, and Silex SD330-AC device, verify the installed firmware version matches the exact build string specified in the Lantronix and Silex advisories before restoring network connectivity — do not rely on self-reported version strings from a device that was potentially compromised via the arbitrary code execution CVEs (CVE-2026-32955, CVE-2026-32956). Monitor syslog output from all patched devices and NetFlow data for management interface traffic for a minimum of 30 days, specifically watching for re-exploitation attempts, unexpected SNMP SET operations, and configuration changes that could indicate a persistent backdoor installed pre-patch. Validate that all serial-attached ICS assets (PLCs, RTUs, meters) are operating at expected baselines via the historian or HMI, as a compromised serial-to-IP converter could have relayed unauthorized commands to downstream equipment before containment.
Forensic Artifacts	Lantronix EDS / Silex SD330-AC syslog output: authentication events (successful and failed logins to web UI and CLI), configuration change events, and firmware flash events — export and hash immediately before patching to establish pre-patch evidentiary baseline. | SNMP traffic logs: UDP 161 captures showing community strings used, OIDs queried or SET, and source IPs — specifically relevant to CVE-2015-5621 (NET-SNMP AgentX heap corruption exploited via crafted SNMP packets) and any CVEs in the BRIDGE:BREAK set targeting SNMP; capture via 'tcpdump -i udp port 161 -w snmp_bridgebreak.pcap'. | HTTP/HTTPS web management access logs from the device or upstream proxy/WAF: look for POST requests to firmware upload endpoints (/upgrade.html, /firmware.cgi), unexpected GET requests to configuration export endpoints, and authentication bypass attempts manifesting as 200 OK responses to unauthenticated requests — directly tied to the authentication bypass CVEs (CVE-2025-67034 through CVE-2025-67038). | Pre-patch firmware image extracted via TFTP or console: binary-diff against known-good vendor firmware using 'binwalk' and 'diff' to detect unauthorized modification consistent with firmware tampering CVEs (CVE-2026-32961, CVE-2026-32963); preserve with SHA-256 hash and chain-of-custody documentation. | NetFlow or firewall session logs for TCP 10001 (Lantronix redirector service): persistent or repeated external connections to this port are a strong indicator of exploitation attempts or established reverse shell channels enabled by the remote code execution vulnerabilities; correlate source IPs against threat intelligence feeds for known ICS-targeting actors.

Per-Action IR Details

Step 1: Containment — Immediately identify all Lantronix EDS3000PS, EDS5000, and Silex SD330-AC devices in your environment. Isolate internet-facing instances by removing direct public internet access; place them behind a firewall or OT DMZ. If isolation is not immediately possible, block inbound access on management ports (typically TCP 80, 443, 23, 161/UDP) at the perimeter.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 — not in IG1 reference, use CIS 4.5 (Implement and Manage a Firewall on End-User Devices) as proxy for host isolation, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run a targeted nmap scan against your OT subnet to fingerprint Lantronix and Silex devices by banner and open port profile: 'nmap -sV -p 23,80,443,161,3001,10001 --open /24 -oN bridge_break_scan.txt'.

Lantronix EDS devices expose a characteristic HTTP banner ('Lantronix EDS') on port 80 and a proprietary redirector service on TCP 10001. Use an ACL on a managed switch (e.g., Cisco IOS 'ip access-list extended BLOCK_BRIDGEBREAK deny tcp any host eq 80', repeat for 23/443) if perimeter firewall changes require a change window. Document every device MAC and IP before isolation.

Evidence: Before isolating, capture a full packet dump of any active sessions to/from the device management interface using 'tcpdump -i host -w bridgebreak_prefirewall_$(date +%Y%m%d%H%M).pcap'. Record the current firmware version string from the device HTTP admin page (GET /deviceinfo.html or equivalent) and the SNMP sysDescr OID (1.3.6.1.2.1.1.1.0) via 'snmpget -v2c -c public sysDescr.0' — these confirm pre-patch state and whether the device has already been tampered with. Screenshot or export the current running configuration before any network changes.

Step 2: Detection — Query your asset inventory and network discovery tools for Lantronix EDS and Silex SD330-AC devices. Run Shodan or internal network scans to identify internet-exposed instances. Review firewall and NGFW logs for unexpected inbound connections to serial-to-IP converter management interfaces. Check SIEM for SNMP traffic anomalies referencing CVE-2015-5621-era MIB OIDs. No public IOC patterns (hashes, IPs) are confirmed at this time.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM, use the following targeted queries: (1) Parse firewall or router syslog for inbound connections to Lantronix/Silex IPs on TCP 23, 80, 443, 10001, and UDP 161 using 'grep -E "(23|80|443|161|10001)" /var/log/firewall.log | grep '. (2) For SNMP anomaly detection specific to CVE-2015-5621 (NET-SNMP AgentX heap corruption), query for SNMPv1/v2c traffic from unexpected source IPs: 'tcpdump -r udp port 161 and not src '. (3) Use Shodan CLI ('shodan search "Lantronix EDS" org:') to verify your external exposure. (4) Check for unexpected HTTP POST or GET requests to /upgrade.html, /firmware.cgi, or /config.cgi in web server access logs on the device if accessible via serial console.

Evidence: Pull and preserve: (1) Firewall/NGFW NetFlow or connection logs for all traffic to/from Lantronix and Silex management IPs for the past 90 days — specifically flag any source IPs making repeated connections to TCP 10001 (Lantronix redirector) or TCP 23 (Telnet, default credential exposure). (2) SNMP trap logs and NMS query logs — look for GET/SET requests targeting writable OIDs that would be abused via CVE-2015-5621 (NET-SNMP AgentX subagent registration abuse). (3) If the device supports syslog export, collect all authentication events — failed and successful logins to the web management interface or CLI are key indicators of pre-exploitation reconnaissance.

Step 3: Eradication — Apply vendor-issued patches from Lantronix (for EDS3000PS and EDS5000 series) and Silex (for SD330-AC). Obtain firmware updates directly from the Lantronix support portal (lantronix.com/support) and the Silex Technology support portal. Verify firmware integrity against vendor-provided checksums before deployment. Disable SNMP v1/v2 where not required; if SNMP is required, upgrade to SNMPv3 with authentication.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Before flashing firmware, verify the downloaded binary checksum against the vendor advisory value: 'sha256sum ' (Linux) or 'Get-FileHash -Algorithm SHA256' (PowerShell). If the device was potentially compromised, perform a factory reset via physical console (serial port) before applying patched firmware — do not trust a software-initiated reset on a device with suspected arbitrary code execution exposure (CVE-2026-32955, CVE-2026-32956). To harden SNMP post-patch without an enterprise tool, use the device CLI to disable v1/v2c: on Lantronix EDS devices, navigate to Configuration > Network Services > SNMP and set 'SNMPv3 only'. Document the change with a before/after screenshot as your change record.

Evidence: Before applying firmware: (1) Extract and preserve the current firmware image via TFTP if the device supports it ('tftp -g -r firmware.bin ') as evidence of the pre-patch state and potential tamper. (2) Export the full running configuration (XML or CLI dump) — on Lantronix EDS devices this is available via the web UI at Configuration > Export or via CLI 'show config'. (3) Record the exact firmware version string (visible at System > About or via SNMP OID 1.3.6.1.2.1.1.1.0) to confirm pre-patch version for patch gap documentation. (4) If the device was internet-exposed prior to containment, treat the current firmware as potentially tampered and document chain of custody for the preserved image.

Step 4: Recovery — After patching, confirm firmware version matches vendor-specified patched release for each device. Re-enable managed network access only after patch verification. Monitor affected devices for anomalous command execution, unexpected file uploads, or unauthorized configuration changes for a minimum of 30 days post-remediation. Validate that serial-connected ICS devices are operating within expected parameters.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Post-patch, verify firmware integrity on each device by querying the SNMP sysDescr OID and comparing to the vendor-documented patched version string: 'snmpget -v3 -u -l authPriv -a SHA -A -x AES -X sysDescr.0'. For the 30-day monitoring window without a SIEM, configure the device to forward syslog to a centralized host (even a Raspberry Pi running rsyslog is sufficient) and run a daily cron job: 'grep -iE "(config change|firmware|upload|login fail|unauthorized)" /var/log/lantronix_syslog.log >> /var/log/bridgebreak_anomaly_review.log'. For serial-connected ICS device validation, compare current process values against baseline using the ICS HMI or historian — unexpected set-point changes on equipment connected through the serial converter are a strong indicator of pre-patch compromise.

Evidence: After patching, collect: (1) SNMP sysDescr and firmware version confirmation query output — save as a timestamped text file for audit evidence. (2) A fresh full configuration export post-patch to compare against the pre-patch export using 'diff' — any unexpected retained configuration (e.g., unauthorized SNMP community strings, added user accounts) indicates the device may have been compromised prior to patching. (3) Syslog output from the first 24 hours of re-enabled network access — look for reconnection attempts from external IPs that previously hit the management interface, which would indicate an active threat actor retrying exploitation post-patch.

Step 5: Post-Incident — This disclosure highlights persistent risks from legacy serial-to-IP bridging devices in OT environments: (1) CVE-2015-5621's presence confirms these devices often carry unpatched components for years — implement a formal OT asset lifecycle and patch tracking process; (2) ~20,000 internet-exposed instances indicate insufficient network segmentation is widespread — enforce OT/IT network segmentation with explicit deny-all defaults for serial converter management interfaces; (3) Map control gaps against NIST SP 800-82 (OT security) and ICS-specific MITRE ATT&CK for ICS techniques T0831, T0836, and T0859.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For a 2-person OT security team: (1) Build a Lantronix/Silex-specific asset register in a spreadsheet tracking firmware version, last patch date, serial-connected device identity, and network zone — update after each maintenance window. (2) Create a YARA rule targeting the Lantronix EDS HTTP banner for use with Nmap scripting engine to catch new or re-imaged devices that revert to unpatched firmware: use 'nmap --script http-title -p 80 /24' and flag any result matching 'Lantronix EDS'. (3) Map BRIDGE:BREAK against MITRE ATT&CK for ICS: T0831 (Manipulation of Control) applies to post-compromise serial command injection through the converter; T0836 (Modify

Parameter) applies to unauthorized set-point changes on serial-connected PLCs/RTUs; T0859 (Valid Accounts) applies to authentication bypass CVEs (CVE-2025-67034 through CVE-2025-67038). Retain these mappings in your threat library for future hunting hypotheses.

Evidence: Compile a post-incident evidence package: (1) Pre- and post-patch configuration diffs for all affected devices. (2) Full 90-day network log extract for all management interface traffic to affected device IPs — retain per NIST AU-11 (Audit Record Retention) for a minimum of 1 year given OT incident severity. (3) Shodan historical export (via Shodan API 'shodan host --history') for any internet-exposed devices — this may show the window of external visibility and whether the device appeared in threat actor tooling lists. (4) Lessons-learned documentation noting CVE-2015-5621's 10-year latency in this product line as justification for accelerating OT patch cadence from annual to quarterly.

Detection Guidance

No confirmed public IOCs (malicious IPs, hashes, or exploit payloads) are available at time of this report. Detection should focus on behavioral and asset-level indicators. (1) Asset exposure: Use internal network discovery tools as your primary mechanism to identify Lantronix EDS3000PS, EDS5000, and Silex SD330-AC devices. Supplement with Shodan queries for 'Lantronix EDS' or 'Silex SD330' to verify public exposure. (Note: Shodan results reflect publicly indexed instances only and are not exhaustive.) Cross-reference against your asset inventory. (2) Authentication anomalies: Review management interface logs (HTTP/HTTPS, Telnet) for authentication bypass patterns, repeated access without credential exchange, or access from unexpected source IPs. (3) Firmware integrity: Compare running firmware versions against vendor-published patched versions; unexpected version strings may indicate tampering via CWE-434 file upload exploitation. (4) SNMP anomalies: Alert on SNMP v1/v2 traffic to/from these devices, particularly queries touching system or interface OIDs, relevant to CVE-2015-5621. (5) Command execution: If these devices generate syslog output, alert on unexpected shell command strings or configuration changes not initiated by authorized administrators. (6) Resource exhaustion: Monitor for device unresponsiveness or management interface unavailability, which may indicate CWE-400 exploitation.

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1046** — Network Service Discovery
- **T1542** — Pre-OS Boot
- **T0831** — Manipulation of Control
- **T1190** — Exploit Public-Facing Application
- **T1068** — Exploitation for Privilege Escalation
- **T0836** — Modify Parameter
- **T1021** — Remote Services
- **T1499** — Endpoint Denial of Service
- **T1059** — Command and Scripting Interpreter
- **T0859** — Valid Accounts
- **T1040** — Network Sniffing

- **T1210** — Exploitation of Remote Services
- **T1565** — Data Manipulation

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **SC-5** — Denial-of-Service Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design
- **A01:2021** — Broken Access Control
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **13.8** — Deploy a Network Intrusion Prevention Solution
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1046	Network Service Discovery	Discovery
T1542	Pre-OS Boot	Defense-Evasion
T0831	Manipulation of Control	Impact
T1190	Exploit Public-Facing Application	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T0836	Modify Parameter	Impair-Process-Control
T1021	Remote Services	Lateral-Movement
T1499	Endpoint Denial of Service	Impact
T1059	Command and Scripting Interpreter	Execution
T0859	Valid Accounts	Persistence
T1040	Network Sniffing	Credential-Access
T1210	Exploitation of Remote Services	Lateral-Movement
T1565	Data Manipulation	Impact

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/22-bridgebreak-flaws-expose-20000...	T3
CVE-2026-32961 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-32961	T1

Source	URL	Tier
CVE-2026-32955 | Tenable®	https://www.tenable.com/cve/CVE-2026-32955	T3
Security Update Guide - Microsoft - Release Notes	https://msrc.microsoft.com/update-guide/releaseNote/2026-Apr	T1
March 2026 CVE Landscape: 31 High-Impact Vulnerabilities ...	https://www.recordedfuture.com/blog/march-2026-cve-landscape	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-32955, CVE-2026-32956, CV...	T1

Generated 2026-04-21 18:38 UTC by TJS Security Command Center