INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 06:39 UTC

20 Vulnerabilities Discovered in Lantronix and Silex Serial-to-IP Converters Exposing OT and Healthcare Systems

SECURITY ANALYSIS | HIGH | CVSS 8.1

SCC Item ID	SCC-STY-2026-0071
Type	Security Analysis
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Lantronix serial-to-IP converter devices; Silex serial-to-IP converter devices (specific model numbers and firmware versions not confirmed from available sources)
Discovery Source	Gemini

Executive Summary

Researchers have identified approximately 20 vulnerabilities across serial-to-IP converter products from Lantronix and Silex Technology, devices that bridge legacy serial equipment to modern IP networks in OT, industrial control, and healthcare environments. Successful exploitation could allow remote attackers to access or manipulate downstream devices, including PLCs, SCADA systems, and medical equipment, without authentication. The findings signal a broader, systemic failure in lifecycle management and patching for a class of infrastructure devices that organizations routinely overlook because they are treated as passive connectors rather than network-accessible attack surfaces.

Technical Analysis

Serial-to-IP converters occupy a deceptively high-risk position in OT and healthcare architectures. They sit between legacy serial devices, typically RS-232 or RS-485 equipment that was never designed for network exposure, and modern IP infrastructure. When compromised, they do not just expose themselves; they expose everything downstream. The approximately 20 vulnerabilities identified across Lantronix and Silex products span weakness classes consistent with the reported CWEs: missing authentication for critical functions (CWE-306), OS command injection (CWE-78), classic buffer overflows (CWE-120), improper authentication (CWE-287), and hardcoded credentials (CWE-798). This combination is particularly dangerous in OT contexts because it maps directly to remote exploitation without prior access, command execution, and persistent backdoor establishment. The MITRE ATT&CK techniques cited, T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1059 (Command and Scripting Interpreter), T1565 (Data Manipulation),

and T1499 (Endpoint Denial of Service), trace a plausible kill chain from initial access through impact. An attacker targeting a healthcare network, for example, could exploit an unauthenticated management interface (T1190/T1133) to reach a serial-connected infusion pump controller or patient monitoring gateway, execute commands via an injected shell (T1059), and either manipulate device behavior (T1565) or deny service to clinical equipment (T1499). Dark Reading characterizes the issue as serial-to-IP devices hiding thousands of old and new bugs - a framing that highlights the broader product category risk: deferred patching, long deployment lifespans, and minimal security scrutiny during procurement. Many of these devices run embedded firmware that vendors rarely update and operators rarely replace, creating a persistent vulnerability window that is difficult to close without device retirement. Specific CVE identifiers, CVSS vectors, and granular technical proof-of-concept details are not confirmed from the available sources. The qualitative severity rating of high and the estimated CVSS base of 8.1 should be treated as preliminary until vendor advisories or a primary research disclosure are published. Security teams should not wait for that confirmation before assessing exposure.

Action Checklist

1. Step 1: Assess exposure, audit your OT, ICS, and healthcare network segments for Lantronix and Silex serial-to-IP converter devices; include asset management systems, network discovery scans, and procurement records, since these devices are frequently undocumented
2. Step 2: Review controls, verify that serial-to-IP converters are isolated behind dedicated OT network segments or VLANs with no direct internet exposure; confirm that management interfaces are not reachable from corporate or guest networks; validate that default or hardcoded credentials (CWE-798) have been changed where firmware permits
3. Step 3: Update threat model, add serial-to-IP converter compromise as an initial access vector in your OT and healthcare threat models; map T1190 and T1133 to these device classes and confirm detection coverage exists for unexpected outbound connections or management interface access from unauthorized hosts
4. Step 4: Communicate findings, brief OT engineering, biomedical engineering (for healthcare), and leadership on the specific risk that legacy serial device bridges represent; frame it as a supply chain and lifecycle management gap, not just a patch problem, since firmware updates may not be available for all affected models
5. Step 5: Monitor developments, track Lantronix and Silex vendor security advisories, CISA ICS-CERT advisories (ics-cert.cisa.gov), and the primary research disclosure for specific CVE assignments, CVSS scores, and patch availability; set alerts for any CISA KEV additions related to these vendors

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and OT/ICS incident response lead if network monitoring identifies any unauthorized connection to a Lantronix or Silex management interface (TCP/9999, TCP/10001, TCP/14000, TCP/23) from a non-OT host, if any downstream PLC, SCADA node, or medical device exhibits unexpected command sequences or state changes coinciding with converter traffic anomalies, or if a healthcare organization's biomedical team identifies unexpected behavior in serial-connected medical devices — the last condition may additionally trigger FDA Medical Device Reporting (MDR) obligations and HIPAA breach notification assessment if PHI is accessible through compromised medical equipment.
Recovery Notes	Post-containment, do not restore serial-to-IP converters to production until firmware has been updated to a patched version (where available) or compensating network controls (ACLs blocking all non-authorized management access, syslog forwarding active, and credential rotation confirmed) are documented and validated — restoring an isolated but unpatched converter to an unrestricted network segment restores the full attack surface. Monitor all identified Lantronix/Silex devices and their downstream serial-connected assets for a minimum of 30 days post-containment, specifically watching for unexpected serial command injection patterns in Zeek or NetFlow logs that would indicate pre-containment compromise of a downstream PLC or medical device that persists after the converter was isolated. For any converter where pre-compromise cannot be ruled out based on log gaps or absence of historical monitoring, treat the downstream serial device (PLC, medical equipment) as potentially tampered and coordinate with OT engineering or biomedical engineering for a physical configuration integrity verification before returning it to service.
Forensic Artifacts	Lantronix/Silex device syslog output (forwarded to central collector): authentication events, management interface login attempts, and serial port connection/disconnection events — specifically look for authentication successes from unexpected source IPs, which would indicate exploitation of a credential vulnerability (CWE-798 hardcoded credentials or authentication bypass) among the ~20 disclosed flaws | Network flow records (NetFlow/IPFIX or Zeek conn.log) for TCP/9999 (Lantronix DeviceInstaller), TCP/10001 (Lantronix raw serial tunnel), and TCP/14000 (Silex management) covering the 90 days prior to this advisory — unexpected inbound connections from internet-routable IPs or corporate network segments indicate exploitation attempts predating public disclosure | Serial tunnel payload captures (Wireshark/tcpdump on the OT network SPAN port, filtered on the converter's IP and serial tunnel port) — an attacker exploiting unauthenticated serial access would generate raw serial protocol frames (Modbus, DNP3, HL7, or proprietary PLC protocols depending on the downstream device) traversing the IP network that would be anomalous in timing, source, and command content relative to the legitimate engineering workstation baseline | Firmware integrity verification output: extract the current firmware image from each Lantronix/Silex device via TFTP or HTTP export and compute its SHA-256 hash, then compare against the hash published in the vendor's release notes — a mismatch indicates firmware tampering, which is a high-confidence indicator of deep device compromise requiring physical replacement rather than software remediation | Downstream device audit logs and state snapshots: for PLCs, export the current ladder logic or function block program and compare against the last known-good backup; for medical devices, obtain the device configuration report and compare against the manufacturer's baseline — unauthorized serial command injection through a compromised converter may have altered device programming or configuration without generating any alert on the IT/OT network

Per-Action IR Details

Step 1: Assess exposure — audit your OT, ICS, and healthcare network segments for Lantronix and Silex serial-to-IP converter devices; include asset management systems, network discovery scans, and

procurement records, since these devices are frequently undocumented

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing asset visibility and IR readiness before an incident is declared

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires knowing what assets are in scope, NIST SI-5 (Security Alerts, Advisories, and Directives) — receipt of advisory triggers asset identification obligation, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must include OT/ICS assets with network exposure, CIS 1.2 (Address Unauthorized Assets) — undocumented serial-to-IP converters constitute unauthorized or unmanaged assets requiring immediate classification

Compensating: Run a passive network scan using nmap with service fingerprinting: 'nmap -sV -p 22,23,80,443,9999,10001,14000 --open -oN lantronix_silex_scan.txt' — Lantronix devices commonly expose TCP/9999 (DeviceInstaller) and TCP/10001 (raw serial tunnel), while Silex devices often expose TCP/14000. Cross-reference nmap output against MAC OUI prefixes: Lantronix OUI block starts with 00:20:4A; Silex Technology uses 00:80:92. For procurement gap-fill, query purchasing systems or CMDB exports with vendor keyword filters 'Lantronix' and 'Silex' going back 10 years given typical OT device lifecycles.

Evidence: Before scanning, capture a passive baseline from your OT network tap or managed switch SPAN port using Wireshark or tcpdump filtered on Lantronix/Silex OUI MACs and their characteristic ports (TCP/9999, TCP/10001, TCP/14000, UDP/30718 for Lantronix DeviceInstaller discovery protocol) — this establishes a pre-remediation traffic baseline that documents which downstream serial devices (PLCs, SCADA nodes, medical equipment) are actively communicating through each converter, critical for impact scoping if exploitation is later confirmed.

Step 2: Review controls — verify that serial-to-IP converters are isolated behind dedicated OT network segments or VLANs with no direct internet exposure; confirm that management interfaces are not reachable from corporate or guest networks; validate that default or hardcoded credentials (CWE-798) have been changed where firmware permits

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolating affected systems to prevent further access while preserving operational continuity

Controls: NIST IR-4 (Incident Handling) — containment actions executed as part of incident handling capability, NIST SC-7 (Boundary Protection) — enforce boundary controls isolating serial-to-IP converters from corporate and internet-facing segments, NIST IA-5 (Authenticator Management) — hardcoded or default credentials (CWE-798) on Lantronix/Silex devices must be rotated or mitigated where firmware supports it, NIST CM-7 (Least Functionality) — disable management interfaces (Telnet, HTTP) on Lantronix/Silex converters that are not operationally required, CIS 4.4 (Implement and Manage a Firewall on Servers) — apply ACLs or firewall rules blocking inbound access to converter management ports from all non-OT segments, CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software) — enumerate and remediate default credentials on all identified Lantronix and Silex devices

Compensating: For teams without NAC or firewall automation: (1) On managed switches, apply port-level ACLs blocking TCP/23 (Telnet), TCP/80 (HTTP management), and TCP/9999 from all VLANs except the designated OT management VLAN — document the ACL change with a change ticket referencing this advisory. (2) To test credential posture without enterprise tooling, use Hydra or Medusa against known Lantronix default credentials ('admin/PASS', 'admin/[blank]') and Silex defaults from vendor documentation in a controlled, authorized test window: 'hydra -l admin -P /usr/share/wordlists/default_creds.txt http-get /'. (3) Log all management interface access by enabling syslog forwarding on each device to a centralized syslog server (rsyslog on a Linux host is sufficient) before making changes.

Evidence: Before modifying network rules or credentials, export current firewall/ACL rulesets and router ARP tables as evidence of pre-remediation exposure state. On each Lantronix/Silex device where access is possible, download the current configuration file (Lantronix devices typically expose config export via HTTP GET /config or via TFTP; consult device-specific admin guide) — this documents whether management services (Telnet, HTTP, SNMP community strings) were enabled and whether non-default credentials were in use, which is material evidence if exploitation is later confirmed. Capture active TCP sessions from the device's management interface before isolation to identify any unexpected current connections.

Step 3: Update threat model — add serial-to-IP converter compromise as an initial access vector in your OT and healthcare threat models; map T1190 and T1133 to these device classes and confirm detection coverage exists for unexpected outbound connections or management interface access from unauthorized hosts

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: establishing detection capability and analytic baselines for this specific attack surface

Controls: NIST IR-4 (Incident Handling) — incident handling capability must include detection coverage for newly identified attack vectors, NIST IR-5 (Incident Monitoring) — track and document incidents; requires monitoring coverage for this device class to be established, NIST SI-4 (System Monitoring) — extend monitoring to cover serial-to-IP converter management interfaces and downstream serial tunnel traffic, NIST RA-3 (Risk Assessment) — updated threat model constitutes a risk assessment update reflecting newly identified vulnerability classes, CIS 8.2 (Collect Audit Logs) — ensure audit logging is enabled on Lantronix/Silex devices and forwarded to a central collector

Compensating: For T1190 (Exploit Public-Facing Application) detection against these converters without a SIEM: configure syslog on each converter to forward authentication events and connection events to a central rsyslog host, then use a Sigma rule translated to grep/awk to alert on authentication failures or unexpected source IPs accessing management ports. For T1133 (External Remote Services), deploy a Zeek (formerly Bro) sensor on the OT network SPAN port and write a Zeek script to alert on any TCP/9999, TCP/10001, or TCP/14000 connections originating from IP ranges outside the authorized OT management subnet — this catches unauthorized serial tunnel access that would indicate a downstream PLC or medical device is being directly manipulated. Reference MITRE ATT&CK ICS Matrix T0886 (Remote Services) as the ICS-specific analog to T1133 for your OT threat model documentation.

Evidence: Pull historical NetFlow or firewall connection logs (minimum 90 days if retained per NIST AU-11 (Audit Record Retention)) and filter for any prior connections to the management ports (TCP/23, TCP/80, TCP/443, TCP/9999, TCP/14000) of the identified Lantronix/Silex converters from hosts outside the authorized OT management network — this establishes whether exploitation attempts preceded this advisory disclosure. Also review DHCP lease logs for unexpected new devices appearing in OT VLANs, which could indicate a threat actor has already pivoted through a compromised converter to place an implant on the network segment hosting downstream PLCs or medical devices.

Step 4: Communicate findings — brief OT engineering, biomedical engineering (for healthcare), and leadership on the specific risk that legacy serial device bridges represent; frame it as a supply chain and lifecycle management gap, not just a patch problem, since firmware updates may not be available for all affected models

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned and structural improvement; this step addresses the systemic lifecycle management failure that produced this exposure

Controls: NIST IR-6 (Incident Reporting) — report findings to appropriate organizational personnel including OT/biomedical stakeholders, NIST IR-8 (Incident Response Plan) — IR plan must be updated to incorporate serial-to-IP converter device classes as a recognized attack surface, NIST SA-22 (Unsupported System Components) — devices for which firmware updates are unavailable constitute unsupported components requiring documented risk acceptance or replacement planning, NIST SI-2 (Flaw Remediation) — where firmware patches are unavailable, document compensating controls as the flaw remediation record, CIS 2.2 (Ensure Authorized Software is Currently Supported) — Lantronix/Silex models without available firmware updates must be flagged as unsupported and scheduled for replacement or isolation, CIS 7.2 (Establish and Maintain a Remediation Process) — risk-based remediation strategy must account for devices where patching is not possible

Compensating: Produce a one-page asset risk register entry for each identified Lantronix/Silex device model that includes: firmware version, patch availability status (confirmed against Lantronix security advisories at lantronix.com/support and Silex advisories at silex.jp/support), downstream devices served (PLC model, medical device, SCADA node), network isolation status, and compensating control in place. For models confirmed to have no firmware fix, document a formal risk acceptance signed by the asset owner or prepare a device replacement request — this record satisfies NIST SI-2 (Flaw Remediation) audit requirements even when patching is impossible. Share the register with biomedical engineering leadership using patient safety impact language where downstream medical

devices are involved, since this may trigger FDA cybersecurity reporting obligations for HDOs.

Evidence: Before the stakeholder brief, compile a complete exposure dossier: (1) list of all identified device models and firmware versions from the asset audit in Step 1, (2) firmware release history from Lantronix and Silex vendor support pages documenting whether security patches have been issued for each model, (3) network diagram or topology export showing each converter's position relative to PLCs, SCADA servers, or medical devices it bridges — this dossier constitutes the factual basis for leadership decisions on risk acceptance vs. replacement and serves as documentation if a downstream incident results in regulatory inquiry.

Step 5: Monitor developments — track Lantronix and Silex vendor security advisories, CISA ICS-CERT advisories (ics-cert.cisa.gov), and the primary research disclosure for specific CVE assignments, CVSS scores, and patch availability; set alerts for any CISA KEV additions related to these vendors

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: maintaining ongoing threat intelligence feeds and advisory monitoring as a standing IR readiness function

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — establish ongoing subscription to CISA ICS-CERT and vendor advisories for Lantronix and Silex as a formal control, NIST IR-4 (Incident Handling) — preparation phase requires maintaining current intelligence on known vulnerabilities affecting in-scope assets, NIST RA-3 (Risk Assessment) — risk assessment must be updated as CVE assignments and CVSS scores are formally published for these ~20 vulnerabilities, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — vulnerability management process must include ICS-CERT advisory tracking for OT device classes, CIS 7.2 (Establish and Maintain a Remediation Process) — remediation process triggers must be tied to KEV additions and CVSS score thresholds for these specific vendor advisories

Compensating: Configure RSS feed monitoring for CISA ICS-CERT advisories (https://www.cisa.gov/cybersecurity-advisories/ics-advisories — RSS available) filtered by 'Lantronix' and 'Silex' keywords using a free feed reader (Feedly free tier or a local rssnix/newsboat instance). For KEV monitoring without a vulnerability management platform, use a daily cron job to curl the CISA KEV JSON catalog and grep for vendor names: 'curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | python3 -c "import json,sys; [print(v) for v in json.load(sys.stdin)[\"vulnerabilities\"] if \"Lantronix\" in str(v) or \"Silex\" in str(v)]"'. Set a calendar reminder to manually check Lantronix (lantronix.com/support/security-advisory/) and Silex (silex.jp/support) advisory pages weekly until all ~20 CVEs are formally assigned and patch status is confirmed.

Evidence: Establish a dated intelligence log capturing: (1) the original research disclosure document or preprint (preserve a local copy since researcher disclosures can be taken down or modified), (2) screenshots of Lantronix and Silex support pages as of today showing current firmware versions and absence/presence of security advisories, and (3) a snapshot of the CISA KEV catalog filtered to both vendors — these time-stamped records establish your organization's knowledge timeline, which is material for incident response documentation if exploitation occurs before patches are available and regulatory or legal questions arise about when the organization became aware of the risk.

Detection Guidance

In the absence of confirmed CVE identifiers or vendor-published indicators, detection should focus on behavioral anomalies consistent with the reported weakness classes. Review firewall and network flow logs for unexpected inbound connections to serial-to-IP converter management ports (commonly TCP 23, 80, 443, 9999, and vendor-specific ports such as Lantronix's DeviceInstaller port 30718). Alert on management interface access from hosts outside designated OT management VLANs. Monitor for serial device traffic anomalies: unexpected command sequences, timing deviations, or protocol errors on downstream serial-connected equipment that could indicate injected commands passing through a compromised converter. For hardcoded credential exposure (CWE-798), audit authentication logs on any converters that support logging; successful logins using default or factory credentials should trigger immediate investigation. If your SIEM ingests OT protocol data (Modbus, DNP3, PROFINET), create detection rules for unexpected write or control commands to

PLCs or SCADA endpoints that are downstream of serial converters. In healthcare environments, biomedical device event logs should be reviewed for anomalous serial command activity. Note: because specific IOCs are not yet published, these detections are behavioral and hypothesis-driven. Revisit and refine when vendor advisories or the primary research disclosure provide concrete indicators.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to SecurityWeek and Dark Reading disclosures for published indicators`	Specific CVE identifiers, payload hashes, and network indicators associated with the Lantronix and Silex vulnerability research have not been confirmed from available secondary sources; primary research publication or vendor advisories are expected to contain concrete indicators	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1565** — Data Manipulation
- **T1059** — Command and Scripting Interpreter
- **T1499** — Endpoint Denial of Service
- **T1133** — External Remote Services

NIST-800-53R5

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

- **SI-16** — Memory Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1565	Data Manipulation	Impact
T1059	Command and Scripting Interpreter	Execution
T1499	Endpoint Denial of Service	Impact
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Serial-to-IP Converter Flaws Expose OT and Healthcare Systems to ...	https://www.securityweek.com/serial-to-ip-converter-flaws-expose-ot...	T3
Serial-to-IP Devices Hide Thousands of Old and New Bugs	https://www.darkreading.com/ics-ot-security/serial-ip-devices-thous...	T3
Researchers found 20 vulnerabilities in Silex and Lantronix serial-to ...	https://x.com/TweetThreatNews/status/2046393506780913957	T3
Serial-to-IP Converter Flaws Expose OT and Healthcare Systems to ...	https://www.show.it/en/serial-to-ip-converter-flaws-expose-ot-and-h...	T3
Serial-to-IP Devices Hide Thousands of Old and New Bugs	https://www.secureitinside.nl/serial-to-ip-devices-hide-thousands-o...	T3

Generated 2026-04-21 06:39 UTC by TJS Security Command Center