BLACKSWAN CYBERSECURITY

THREAT ADVISORY

BRIDGE:BREAK Vulnerabilities in Serial-to-IP Converters

April 23, 2026

Target Sector: Healthcare & Public Health (HPH)
Threat: Unauthenticated RCE, Firmware Tampering, and DoS (BRIDGE:BREAK) Affected
Vendors: Lantronix, Silex (and potentially other serial device server vendors)

Executive Summary

Twenty (20) new vulnerabilities, collectively tracked as BRIDGE:BREAK, have been discovered in serial-to-IP converters manufactured by Lantronix and Silex. These devices are heavily utilized in healthcare environments to connect legacy serial medical equipment to modern IP networks. Threat actors—ranging from extortion groups to state-sponsored hackers—can exploit these flaws to achieve remote code execution, upload malicious firmware, and execute denial-of-service (DoS) attacks, directly impacting patient care and clinical operations.

Municipal Utility Implications

In both power and gas utilities, the serial-to-IP converter is a dangerous choke point. Because these converters sit at the very edge of the network, right before the physical process, compromising them allows an attacker to bypass firewalls and traditional IT/OT security monitoring tools situated higher up in the network architecture. The attacker essentially gains logical proximity to the physical physics of the grid, making the BRIDGE:BREAK vulnerabilities a highly attractive vector for kinetic disruption. Couple this with the increasing global threat to US critical infrastructure, and this should be considered a critical advisory.

Municipal electric grids rely heavily on serial-to-IP converters in electrical substations and distribution networks.

- **Substation "Blindness" (Loss of View)**: By executing a DoS attack or loading malicious firmware on converters, attackers can sever communication between the SCADA master server and substation RTUs. Grid operators would lose real-time visibility into critical metrics like voltage, current, frequency, and transformer temperatures, making it nearly impossible to balance loads or detect localized outages.
- **False Data Injection (Manipulation of View)**: Attackers could intercept and alter serial communications before they are converted to IP traffic. By feeding false telemetry back to the control center (e.g., falsely reporting normal voltage during a surge, or indicating a breaker is closed when it is open), attackers can trick human operators or automated safety systems into making decisions that cascade into broader blackouts or physical equipment damage.

- **Loss of Remote Control**: If the converters are taken offline, dispatchers lose the ability to remotely trip or close breakers, manage tap changers, or reroute power. Routine operations and emergency incident response would require dispatching technicians directly to physical substation locations ("rolling trucks"), drastically increasing outage durations.

Impacts on Municipal Natural Gas Utilities

Natural gas distribution networks utilize serial-to-IP converters at gate stations, compressor stations, and along pipeline monitoring points.

- **Pressure and Flow Manipulation**: Serial devices often connect to flow computers and pressure sensors. If an attacker manipulates this telemetry, the SCADA system might incorrectly read pipeline pressure as dropping. Automated systems or operators might respond by increasing pressure via compressors, potentially exceeding the pipeline's Maximum Allowable Operating Pressure (MAOP) and creating a risk of rupture or explosion.
- **Valve Control Disruption**: Remote automated block valves, crucial for shutting off gas flow during a leak or pipeline rupture, often rely on serial-to-IP communication. A DoS attack on these converters would render operators unable to remotely close valves, exacerbating the physical consequences of an incident.
- **Odorization Failures**: Municipal utilities add mercaptan (the "rotten egg" smell) to natural gas at city gate stations so leaks can be detected by the public. The injection systems are often monitored and controlled via legacy serial connections. Tampering with these systems could result in un-odorized gas entering the municipal distribution network, significantly raising the risk of undetected residential or commercial leaks.

Healthcare Sector Implications

Serial-to-IP converters are often the invisible "glue" holding clinical networks together. Exploitation of the BRIDGE:BREAK vulnerabilities allows attackers to silently manipulate data or cause severe disruptions to critical medical workflows. **Demonstrated impacts in healthcare environments include**:

- **Laboratory Processing Backlogs**: Analyzers can be forced to stop reporting results to Laboratory Information Systems (LIS), severely delaying diagnoses.
- **Operating Room Disruption**: Surgical lighting controllers and environmental sensors can become unresponsive to remote commands, creating hazardous conditions during procedures.

- **Patient Monitoring Failures**: Patient telemetry monitors can lose network connectivity, blinding nursing staff to critical shifts in patient vitals.
- **Equipment Calibration Halts**: Workflows for infusion pump calibration and certification can be disrupted or halted entirely.
- **Data Manipulation**: Attackers can manipulate medical telemetry and sensor readings in transit to conceal dangerous conditions from human operators.

Threat Actor TTPs (Tactics, Techniques, and Procedures)

While specific IOCs (like malware hashes) depend on the individual threat actor utilizing the exploit, the underlying execution path maps to the following MITRE ATT&CK framework TTPs:

- Reconnaissance (TA0043):
  - *T1596 - Search Open Technical Databases:* Threat actors use Shodan and open-source intelligence (OSINT) to identify internet-exposed serial-to-IP converters, pinpointing internal IP addresses, vendor names, and associated facility context.
- Initial Access (TA0001):
  - *T1190 - Exploit Public-Facing Application:* Exploiting unauthenticated vulnerabilities on devices improperly exposed directly to the internet.
  - *T1078 - Valid Accounts:* Leveraging default or weak administrative credentials on the converters.
- Execution (TA0002):
  - *T1059.004 - Command and Scripting Interpreter: Unix Shell:* Utilizing OS command injection vulnerabilities within the BRIDGE:BREAK chain to execute arbitrary commands on the converter's underlying operating system.
- Defense Evasion (TA0005):
  - *T1542.001 - System Firmware:* Bypassing authentication to upload arbitrary files and tamper with the device’s firmware, embedding persistence or executing destructive payloads.
- Impact (TA0040):
  - *T1498 - Network Denial of Service:* Deploying weaponized firmware to cause the converters to permanently stop responding on the network, effectively cutting off the medical devices from the hospital network.
  - *T1565.002 - Data Manipulation: Transmitted Data Manipulation:* Intercepting and altering serial data (such as sensor telemetry or lab results) as it is converted to IP traffic.

THREAT ADVISORY

BRIDGE:BREAK Vulnerabilities in Serial-to-IP Converters

April 23, 2026

Mitigation and Remediation Recommendations

Healthcare organizations are urged to take the following actions immediately to secure their clinical environments:

1. **Identify and Inventory**: Conduct a comprehensive sweep of the network to identify all serial-to-IP converters/serial device servers. Look specifically for Lantronix, Silex, Moxa, Digi, Advantech, and Perle devices connected to laboratory equipment, environmental controls, and patient monitors.
2. **Remove Internet Exposure**: Ensure that no serial-to-IP converter is directly accessible from the public internet. Access should be strictly gated behind firewalls and VPNs.
3. **Apply Vendor Patches**: Both Lantronix and Silex have released patches addressing the BRIDGE:BREAK vulnerabilities. Review advisories from CISA and the respective vendors, and patch devices during standard clinical maintenance windows.
4. **Network Segmentation**: Isolate serial-to-IP converters and the legacy medical devices they support into dedicated, tightly controlled VLANs. Implement strict firewall rules limiting communication only to the specific internal servers (e.g., the LIS) they require.
5. **Monitor for Anomalous Activity**: Monitor network traffic for unauthorized attempts to access the management interfaces of these converters, or unusual spikes in traffic that could indicate firmware uploads or OS command injection attempts.

Contact Blackswan Cybersecurity at 855-BLK-SWAN or Contact@Blackswancybersecurity.com