INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 13:39 UTC

Serial-to-IP Converters Expose OT Networks Through Legacy Protocol Gaps and Unpatched Firmware

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0072
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Lantronix and other serial-to-IP converter devices (20,000+ internet-exposed units identified; specific vendor models per Forescout BRIDGE:BREAK research)
Published	2026-04-20T17:00:00
Discovery Source	Rss

Executive Summary

Forescout Research Labs disclosed BRIDGE:BREAK, a set of 22 vulnerabilities across serial-to-IP converter devices from Lantronix and other vendors, with more than 20,000 units exposed directly to the internet. These devices sit at the boundary between legacy industrial serial networks and modern IP infrastructure, meaning successful exploitation could allow attackers to gain unauthorized access, execute commands, or move laterally into OT, ICS, and healthcare environments without triggering standard IT security controls. The disclosure reinforces a persistent and widening gap: critical infrastructure organizations have modernized their IT perimeters while leaving decades-old operational technology exposed with default credentials, unencrypted communications, and no authentication on critical functions.

Technical Analysis

BRIDGE:BREAK represents one of the more structurally significant OT disclosures in recent memory, not because of a single critical zero-day, but because of what the vulnerability classes reveal about the state of serial-to-IP device security across the board. Forescout identified 22 distinct vulnerabilities spanning five weakness categories: default or hardcoded credentials (CWE-1392), OS command injection (CWE-78), stack-based buffer overflow (CWE-121), missing encryption of sensitive data (CWE-311), and missing authentication for critical functions (CWE-306). Each class represents a foundational security control that was never implemented or was abandoned in firmware that has not been meaningfully updated.

The attack surface is defined by the device's purpose. Serial-to-IP converters translate RS-232 and RS-485 serial protocols, the communication standards that run programmable logic controllers, sensors, meters, and medical equipment, into IP traffic routable across modern networks. That translation function is precisely what makes them valuable to operations teams and dangerous as an attack entry point. An attacker who compromises one of these devices does not land in a traditional IT environment where EDR, SIEM telemetry, and network segmentation provide layered defense. They land in a protocol environment where traffic is largely unmonitored, devices rarely authenticate to one another, and lateral movement maps to MITRE ATT&CK for ICS techniques including T0866 (Exploitation of Remote Services), T0813 (Denial of Control), T0822 (Exploit Public-Facing Application), and T0831 (Manipulation of Control).

Forescout's internet exposure count of more than 20,000 devices is the operational measure that elevates this from a research finding to an active risk. Devices reachable from the public internet with default or hardcoded credentials (T1078.001) and no authentication on management functions (T1190) require no insider access, no supply chain compromise, and no advanced tradecraft to reach. Command injection flaws (T1059) and buffer overflows (CWE-121) provide code execution paths once initial access is established. Missing encryption (CWE-311) enables passive interception of serial communications in transit (T1040), which in a healthcare environment could expose patient device telemetry or infusion pump commands.

The broader pattern Forescout identifies is consistent with findings from CISA advisories on ICS device security: legacy serial protocol devices were designed for isolated environments and have been connected to IP networks without the security controls that IP-connected devices require. Firmware update mechanisms are frequently absent, difficult to use, or dependent on vendor support cycles that do not match the operational lifespans of the equipment. Organizations in manufacturing, energy, water, and healthcare have been running these devices for years, sometimes decades, with no patch cadence and no visibility into whether they are internet-exposed.

The MITRE ATT&CK for ICS mapping across this disclosure, spanning initial access, execution, lateral movement, impair process control, and inhibit response function, describes a complete intrusion chain, not a theoretical one. Security teams should treat BRIDGE:BREAK as a prompt to audit serial-to-IP converter inventory rather than wait for exploitation evidence.

Action Checklist

1. Step 1: Assess exposure, inventory all serial-to-IP converter devices in your environment, prioritizing Lantronix and other vendors named in the Forescout BRIDGE:BREAK research; identify which units are internet-facing using your asset management system and corroborate with a Shodan or Censys search scoped to your IP ranges
2. Step 2: Eliminate default and hardcoded credentials immediately, audit all identified devices for factory-default or hardcoded credentials (CWE-1392, T1078.001); replace with unique strong credentials where firmware permits; where it does not, document and escalate to vendor or isolation priority
3. Step 3: Segment and firewall, remove serial-to-IP converter devices from direct internet exposure; place them behind a dedicated OT DMZ or industrial firewall; restrict management interface access to defined jump hosts or OT management VLANs; apply zero-trust network access principles where feasible
4. Step 4: Apply vendor firmware updates, contact Lantronix and other affected vendors for patched firmware releases tied to BRIDGE:BREAK; establish a tracking record for each device model and firmware version; where patches are unavailable, apply compensating controls documented under CISA's ICS security guidance

5. Step 5: Enable encrypted communications, where device firmware supports TLS or SSH for management, enforce it; where unencrypted serial-over-IP is unavoidable, document it as a residual risk and restrict network paths to prevent interception
6. Step 6: Update threat model, add serial-to-IP converter devices as a tracked asset class in your threat register; map coverage against MITRE ATT&CK for ICS techniques T0866, T0822, T0813, T0831, and T0883; identify detection gaps in OT network monitoring
7. Step 7: Communicate findings, brief operational technology leads, facility managers, and relevant business owners on device inventory findings and remediation timelines; brief CISO and risk committee on internet-exposed unit count and segmentation gaps with specific remediation milestones
8. Step 8: Monitor for exploitation, track CISA ICS advisories and Forescout research updates for BRIDGE:BREAK exploitation evidence; monitor OT network traffic for anomalous serial protocol behavior, unexpected management interface access, and lateral movement indicators described in the Forescout disclosure

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO, legal counsel, and sector-specific regulatory authorities if any BRIDGE:BREAK-affected device with confirmed default or hardcoded credentials is found to have had unauthorized external connections in firewall/NetFlow logs, or if any device connects to systems processing PHI, operational control functions in critical infrastructure (energy, water, manufacturing), or is subject to NERC CIP, HIPAA, or equivalent regulatory scope — the combination of internet exposure, 20,000+ affected units, and OT/ICS blast radius meets the threshold for mandatory incident reporting in multiple regulated sectors.
Recovery Notes	After segmentation and firmware patching are complete, re-validate each serial-to-IP device's management interface is unreachable from outside the OT management VLAN using an nmap scan from an external vantage point, and verify serial protocol sessions are operating within baseline function code ranges using Zeek or Wireshark captures. Monitor OT network traffic for a minimum of 30 days post-remediation for delayed persistence indicators — specifically unexpected outbound connections from serial-to-IP device IPs, which could indicate pre-existing implants surviving a firmware update if the update did not perform a full factory reset. Establish a quarterly firmware review cadence for this device class given the Forescout BRIDGE:BREAK research indicates this vendor category has historically lacked a mature vulnerability disclosure and patching program.

Forensic Artifacts	Firewall and NetFlow session logs for the prior 90 days filtered to destination IPs of all identified serial-to-IP converter devices on TCP/9999, TCP/23, TCP/80, TCP/443, and UDP/30718 — connection attempts from external IPs to these ports constitute direct exploitation attempt evidence for BRIDGE:BREAK vulnerability classes | Lantronix device syslog output (if syslog forwarding was enabled) showing authentication events, configuration changes, and service state changes — unexpected configuration writes from non-jump-host IPs indicate unauthorized access consistent with CWE-1392 default credential exploitation | Wireshark PCAP captures from OT DMZ SPAN ports showing serial-over-IP session content — out-of-baseline Modbus or DNP3 function codes (particularly FC 8, FC 43, DNP3 Direct Operate commands) during periods not corresponding to authorized operational activity are indicators of T0831 (Manipulation of Control) exploitation | nmap banner grab output capturing firmware version strings and open service ports per device IP at time of discovery — this establishes which specific BRIDGE:BREAK CVEs applied to each device and anchors the breach window timeline for incident reporting | Shodan/Censys historical exposure records for your IP ranges showing when each serial-to-IP device first appeared as internet-accessible — Shodan's historical data (available via API) can establish the internet exposure window, which is critical for determining regulatory notification timelines and breach scope under HIPAA or sector-specific ICS reporting requirements

Per-Action IR Details

Step 1: Assess exposure — inventory all serial-to-IP converter devices in your environment, prioritizing Lantronix and other vendors named in the Forescout BRIDGE:BREAK research; identify which units are internet-facing using your asset management system and corroborate with a Shodan or Censys search scoped to your IP ranges

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR Capability and Asset Visibility

Controls: NIST IR-4 (Incident Handling), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Run a Shodan CLI query scoped to your ASN or IP CIDR: `shodan search 'lantronix' net:YOUR.CIDR.BLOCK` and cross-reference with `censys search 'lantronix' --index=hosts`. Locally, use nmap with service fingerprinting: `nmap -sV -p 23,80,443,9999,30718 --script banner ` — Lantronix DeviceInstaller default ports include TCP/9999 and TCP/30718. Export results to a CSV and diff against your CMDB. A two-person team can complete a /16 scan in under 2 hours with nmap's -T4 timing.

Evidence: Before modifying any device or network configuration, snapshot: (1) Shodan/Censys search results with timestamps for your IP ranges showing exposed Lantronix or BRIDGE:BREAK-affected devices; (2) nmap scan output showing open management ports (TCP/9999, TCP/23, TCP/80, TCP/443) per device IP; (3) current firmware version strings captured via banner grabbing (`nmap --script banner`) — these establish the pre-remediation baseline and are required for gap analysis against Forescout's affected firmware version list.

Step 2: Eliminate default and hardcoded credentials immediately — audit all identified devices for factory-default or hardcoded credentials (CWE-1392, T1078.001); replace with unique strong credentials where firmware permits; where it does not, document and escalate to vendor or isolation priority

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management) — implied via CWE-1392 hardcoded credential remediation, CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords)

Compensating: Pull Lantronix default credential lists from the vendor's published documentation and cross-reference against the Forescout BRIDGE:BREAK disclosure appendix for hardcoded credential CVEs. Attempt login to each device's web management interface (TCP/80 or TCP/443) and CLI (TCP/23 or TCP/9999) using known defaults (e.g., Lantronix default: user `admin`, password blank or `PASS`). Document each result in a spreadsheet: device IP, model, firmware, credential status (default/hardcoded/changed/unknown). For devices where firmware prohibits credential change, immediately flag for VLAN isolation — this is your prioritized isolation list.

Evidence: Before changing any credentials: (1) capture a screenshot or curl output of the device's web management login page confirming default credential acceptance — this is evidence of CWE-1392 exposure and establishes breach window for incident timeline; (2) capture syslog or management interface session logs from the device if accessible, showing any prior authentication events; (3) check upstream network device (firewall/switch) logs for prior connections to device management ports from external IPs — on pfSense/OPNsense, review firewall state table logs filtered to TCP/9999 and TCP/23 destined to the serial-to-IP device IPs.

Step 3: Segment and firewall — remove serial-to-IP converter devices from direct internet exposure; place them behind a dedicated OT DMZ or industrial firewall; restrict management interface access to defined jump hosts or OT management VLANs; apply zero-trust network access principles where feasible

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: On pfSense/OPNsense or iptables-based firewalls, create an explicit deny-all rule for inbound traffic to the serial-to-IP device subnet from any WAN or untrusted interface. Then add permit rules exclusively for the jump host IP(s) to TCP/9999, TCP/23, and TCP/80 on each device. Example iptables rules: `iptables -I FORWARD -d -j DROP` followed by `iptables -I FORWARD -s -d -j ACCEPT`. Validate with a port scan from a non-jump-host IP confirming all management ports are unreachable. Document the pre- and post-segmentation network diagram as an incident record artifact.

Evidence: Before implementing segmentation changes: (1) export the current firewall ruleset and routing table as a timestamped baseline — this documents the pre-remediation exposure window; (2) capture NetFlow or firewall session logs for all connections to serial-to-IP device IPs for the prior 90 days — on pfSense, export from Status > System Logs > Firewall filtered to destination IPs of your device inventory; (3) on managed switches, capture the MAC address table and ARP cache for OT segments to identify any unknown hosts that may have already gained adjacency to these devices via T0819 (Exploit Public-Facing Application) activity.

Step 4: Apply vendor firmware updates — contact Lantronix and other affected vendors for patched firmware releases tied to BRIDGE:BREAK; establish a tracking record for each device model and firmware version; where patches are unavailable, apply compensating controls documented under CISA's ICS security guidance

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Removing Vulnerabilities from the Environment

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Obtain firmware binaries directly from Lantronix support portal (support.lantronix.com) and validate SHA-256 checksums against vendor-published hashes before flashing — do not source firmware from third-party mirrors. For devices awaiting patches, implement CISA ICS-CERT compensating controls per Advisory ICSA-series guidance: disable unused services (Telnet/TCP/23, HTTP/TCP/80) via the device CLI where supported, restrict SNMP community strings from defaults, and disable DeviceInstaller broadcast discovery (UDP/30718) at the network perimeter. Track each device model, current firmware, target firmware, and patch status in a spreadsheet updated weekly until all units reach patched state.

Evidence: Before applying firmware: (1) capture current firmware version via the device web UI or CLI (`show version` or equivalent Lantronix command) and store as a signed record — this establishes the pre-patch vulnerability window for regulatory reporting; (2) if any device shows a firmware version not in your records, treat as a potential tamper

indicator and preserve a full device configuration export before proceeding; (3) after patching, re-run nmap banner grabbing against the device to confirm version string change and log the delta as your patch verification record per NIST SI-2 (Flaw Remediation) requirements.

Step 5: Enable encrypted communications — where device firmware supports TLS or SSH for management, enforce it; where unencrypted serial-over-IP is unavoidable, document it as a residual risk and restrict network paths to prevent interception

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Hardening to Prevent Recurrence

Controls: NIST SC-8 (Transmission Confidentiality and Integrity), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 3.6 (Encrypt Data on End-User Devices), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For devices supporting SSH, disable Telnet and enforce SSH-only management: on Lantronix devices, this is configurable via the web UI under Services > Telnet/SSH or equivalent CLI command `set service telnet disable`. Verify with `nmap -sV -p 23 ` confirming TCP/23 is closed. For serial-over-IP traffic that cannot be encrypted (e.g., legacy Modbus or DNP3 tunneled over TCP), use Wireshark on the OT DMZ mirror port to capture a baseline traffic sample and verify no management credentials are transmitted in plaintext on the serial data channel. Document all residual unencrypted paths in your risk register with a waiver signed by the OT/ICS system owner.

Evidence: Before enforcing encryption changes: (1) capture a Wireshark packet capture on the management VLAN spanning port for 15 minutes during normal operations — filter on `tcp.port==23 or tcp.port==80` to document any plaintext credential transmission occurring over Telnet or HTTP to these devices, which constitutes direct evidence of BRIDGE:BREAK exposure to credential interception; (2) record the TLS version and cipher suite offered by each device's HTTPS interface using `nmap --script ssl-enum-ciphers -p 443 ` — weak TLS configurations are part of the BRIDGE:BREAK vulnerability surface; (3) document which device models lack TLS/SSH support entirely as these require vendor escalation and compensating network controls.

Step 6: Update threat model — add serial-to-IP converter devices as a tracked asset class in your threat register; map coverage against MITRE ATT&CK for ICS techniques T0866, T0819, T0813, T0831, and T0883; identify detection gaps in OT network monitoring

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned and Detection Improvement

Controls: NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment) — implied via threat model update, NIST SI-4 (System Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Map each BRIDGE:BREAK-relevant ATT&CK for ICS technique to your current detection coverage: T0866 (Exploitation of Remote Services) — do you have alerts on unexpected management interface connections to these devices? T0819 (Exploit Public-Facing Application) — do you monitor for reconnaissance scans targeting serial-to-IP ports? T0813 (Denial of Service) — do you have availability monitoring on OT serial links? T0831 (Manipulation of Control) and T0883 (Internet Accessible Device) — are these device IPs in your external attack surface monitoring scope? For each gap, write a Sigma detection rule or osquery scheduled query and document the gap in your threat register. Use the MITRE ATT&CK for ICS Navigator layer to visualize coverage and gaps as a deliverable for the CISO brief in Step 7.

Evidence: For threat model validation: (1) pull historical IDS/IPS or firewall logs filtered to your serial-to-IP device IPs and scan for connection attempts on TCP/9999, TCP/30718, and TCP/23 from external sources — any hits represent prior reconnaissance that should be reviewed against the BRIDGE:BREAK disclosure timeline; (2) review OT network monitoring tool logs (if Claroty, Dragos, or Zeek/Bro on a network tap is deployed) for unusual protocol anomalies on serial-over-IP sessions prior to this disclosure; (3) check DNS query logs from OT segment resolvers for lookups of Lantronix update or management domains — unexpected external DNS from OT devices is a lateral movement indicator consistent with T0883.

Step 7: Communicate findings — brief operational technology leads, facility managers, and relevant business owners on device inventory findings and remediation timelines; brief CISO and risk committee on internet-exposed unit count and segmentation gaps with specific remediation milestones

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Reporting and Stakeholder Communication

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST IR-5 (Incident Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Structure the CISO brief around three data points from Steps 1-3: (1) count of internet-exposed serial-to-IP devices found via Shodan/Censys correlated to your IP ranges; (2) count of devices with default or hardcoded credentials confirmed; (3) count of devices lacking available firmware patches. For OT leads, provide a per-facility table mapping device IP, model, firmware version, exposure status, and remediation action with owner and due date. For regulated environments (healthcare, energy, water), explicitly flag whether any exposed devices connect to systems covered under HIPAA, NERC CIP, or ICS-CERT reporting obligations — this triggers escalation beyond an internal brief.

Evidence: The communication package itself is an IR artifact: (1) retain timestamped copies of all inventory exports, Shodan/Censys search results, and nmap scan outputs from Step 1 as evidence of the scope assessment; (2) retain a copy of the risk acceptance or escalation decision for any device where patching is deferred — this documents due diligence for regulatory purposes; (3) if any device was confirmed internet-exposed with default credentials and connects to a healthcare or critical infrastructure network, preserve all evidence of exposure scope and timeline as this may trigger mandatory reporting under HIPAA Breach Notification Rule or sector-specific ICS incident reporting requirements. Worth noting: if exposed devices connect to systems processing PHI or critical infrastructure control functions, you may want to verify mandatory notification obligations with your legal and compliance counsel.

Step 8: Monitor for exploitation — track CISA ICS advisories and Forescout research updates for BRIDGE:BREAK exploitation evidence; monitor OT network traffic for anomalous serial protocol behavior, unexpected management interface access, and lateral movement indicators described in the Forescout disclosure

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring for Indicators of Compromise

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Zeek (formerly Bro) on a network tap or SPAN port on the OT DMZ segment and write a Zeek script to alert on new TCP connections to device management ports (TCP/9999, TCP/23, TCP/80) from any source other than your defined jump host IPs. For serial-over-IP protocol monitoring, capture baseline Modbus/DNP3 traffic with Wireshark during normal operations and use the `modbus` or `dnp3` Wireshark dissectors to establish normal function code ranges — alert on out-of-baseline function codes (e.g., Modbus FC 8 Diagnostics, FC 43 MEI Read Device Identification) that could indicate reconnaissance or manipulation per T0831 and T0866. Subscribe to CISA ICS-CERT advisories via RSS at https://www.cisa.gov/uscert/ics/advisories and set a keyword alert for 'Lantronix' and 'BRIDGE:BREAK' in your threat intel feed.

Evidence: Ongoing monitoring artifacts to preserve: (1) Zeek connection logs (`conn.log`) filtered to serial-to-IP device IPs, retained for minimum 90 days, showing source IP, destination port, bytes transferred, and connection duration — anomalous short high-frequency connections to TCP/9999 are consistent with automated exploitation attempts against BRIDGE:BREAK vulnerabilities; (2) device syslog output (configure syslog forwarding from Lantronix devices to a syslog server if supported) capturing authentication attempts, configuration changes, and service restarts — unexpected reboots may indicate firmware exploitation or denial-of-service per T0813; (3) PCAP files of any anomalous sessions to management ports — preserve full packet captures of any session not originating from a known jump host IP as these are primary forensic evidence of exploitation attempts.

Detection Guidance

Detection for BRIDGE:BREAK exploitation requires visibility at the OT network layer, which many organizations currently lack. Priority hunting and monitoring actions:

Network traffic analysis: Deploy passive OT network monitoring (tools such as Claroty, Dragos, or Nozomi Networks) on segments containing serial-to-IP converters. Look for unexpected management interface access (Telnet, HTTP, SNMP) originating from hosts outside the defined OT management network. Flag any management session not originating from a known jump host.

Credential use anomalies: Query authentication logs for serial-to-IP devices that support logging. Alert on any login using default usernames (commonly 'admin', 'manager', or vendor-specific defaults documented in Lantronix product manuals). Lateral movement using default credentials maps to T1078.001.

Command execution indicators: Where device logging captures shell or CLI activity, alert on OS-level commands that are inconsistent with normal configuration operations. Command injection exploitation (CWE-78, T1059) will surface as unexpected process spawning if the device has sufficient logging capability.

Unencrypted traffic interception: Monitor for unexpected hosts initiating connections to serial-over-IP streams. Passive capture on OT segments can identify hosts receiving serial data they should not be receiving (T1040).

Internet exposure validation: Run recurring Shodan or Censys queries scoped to your organization's IP ranges, specifically filtering for Lantronix device banners and serial-to-IP converter fingerprints. Any result indicating internet-exposed management interfaces warrants immediate investigation.

Log sources to prioritize: OT network flow data, firewall deny/allow logs for OT DMZ segments, SNMP trap logs from serial-to-IP devices, and any syslog output the devices support. Most legacy serial-to-IP converters have limited native logging; compensate with network-layer visibility.

Hunting hypothesis: Search for any new or unexpected IP address communicating with serial-to-IP converter management ports (TCP 23, 80, 443, 161) over the past 30 days. Cross-reference against asset inventory and authorized management host lists.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to Forescout Research Labs BRIDGE:BREAK disclosure at forescout.com/research-labs/bridgebreak-vulnerabilities-thrive-in-serial-to-ethernet-converters/ for published indicators`	Forescout's BRIDGE:BREAK research report is the primary source for specific exploit indicators, affected firmware versions, and device fingerprints; the item data provided does not include extracted IOC values	LOW

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T0866** — Exploitation of Remote Services
- **T0813** — Denial of Control
- **T1562.001** — Disable or Modify Tools
- **T1021** — Remote Services

- **T0819** — Exploit Public-Facing Application
- **T1078.001** — Default Accounts
- **T1040** — Network Sniffing
- **T0883** — Internet Accessible Device
- **T0831** — Manipulation of Control
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(e)(1)** — Transmission Security

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T0866	Exploitation of Remote Services	Initial-Access
T0813	Denial of Control	Impact
T1562.001	Disable or Modify Tools	Defense-Evasion
T1021	Remote Services	Lateral-Movement
T0819	Exploit Public-Facing Application	Initial-Access
T1078.001	Default Accounts	Defense-Evasion
T1040	Network Sniffing	Credential-Access
T0883	Internet Accessible Device	Initial-Access
T0831	Manipulation of Control	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/ics-ot-security/serial-ip-devices-thous...	T3
22 BRIDGE:BREAK Flaws Expose 20000 Lantronix and ...	https://thehackernews.com/2026/04/22-bridgebreak-flaws-expose-20000...	T3
Serial-to-IP Converter Flaws Expose OT and Healthcare ...	https://www.securityweek.com/serial-to-ip-converter-flaws-expose-ot...	T3
Vulnerabilities Thrive in Serial-to-Ethernet Converters	https://www.forescout.com/research-labs/bridgebreak-vulnerabilities...	T3

Source	URL	Tier
Forescout Identifies 22 New Vulnerabilities on Serial-to-IP ...	https://finance.yahoo.com/sectors/technology/articles/bridge-break-...	T3

Generated 2026-04-21 13:39 UTC by TJS Security Command Center