INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 08:40 UTC

Taiwan High-Speed Rail Attack: SDR Exploit of 19-Year-Old TETRA Parameters Halts Four Trains

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0109
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	TETRA communication systems, Taiwan High Speed Rail (THSR) network; TETRA protocol implementations with static/unrotated radio parameters
Published	2026-05-05T13:34:09
Discovery Source	Rss

Executive Summary

On April 5, 2026, a 23-year-old student with consumer-grade radio hardware halted four Taiwan High-Speed Rail trains for 48 minutes by spoofing a TETRA emergency beacon, triggering automatic braking across the network. The attack succeeded because THSR never rotated its TETRA radio parameters across 19 years of operation, a credential management failure that allowed a low-sophistication actor to bypass seven verification layers with off-the-shelf equipment. This incident demonstrates that legacy OT/ICS communication protocols operating on static credentials are viable targets for physical-consequence attacks, and that operational rail and critical infrastructure networks face realistic disruption threats from actors well below nation-state capability.

Technical Analysis

The April 5, 2026 Taiwan High-Speed Rail incident represents a textbook OT physical-consequence attack achieved through protocol exploitation rather than software vulnerability. The attacker, identified as a 23-year-old university student, acquired THSR-specific TETRA radio parameters from a 21-year-old accomplice with apparent insider access. Using consumer-grade software-defined radio (SDR) hardware, he intercepted and decoded network traffic, then transmitted a forged General Alarm beacon that the THSR safety system accepted as legitimate, triggering automatic emergency braking across four trains.

The attack chain maps cleanly to the described CWEs: CWE-798 (static credentials never rotated in 19 years), CWE-287 (the network accepted a spoofed beacon without adequate authentication), and CWE-284 (no detection mechanism flagged an unregistered transmitter on the network). On the MITRE ICS ATT&CK side, the

incident aligns with T0855 (Unauthorized Command Message) and T0803 (Block Command Message) for the OT-layer impact, with T1040 (Network Sniffing) and T1602 (Data from Configuration Repository) explaining how parameters were harvested, and T1200 (Hardware Additions) reflecting the SDR's role as the access vector.

The TETRA protocol's structural weaknesses were established prior to this incident. The TETRA:BURST research, published in 2023 by Midnight Blue and presented at Black Hat USA 2023, documented multiple cryptographic and implementation flaws in TETRA affecting critical infrastructure communications globally, including law enforcement and rail networks. That research corroborates the protocol-level exposure surface that made this specific attack feasible. What THSR's incident adds to that earlier body of work is the demonstration that even without exploiting a discrete software vulnerability, static parameter management alone is sufficient to enable a low-sophistication actor to produce physical rail disruption.

The involvement of an insider-adjacent accomplice who supplied THSR-specific parameters is a material detail for defenders. The attacker did not need to independently crack TETRA encryption; he received the keys. This shifts the primary defensive gap from cryptographic hardness to insider threat controls, parameter rotation discipline, and radio network monitoring. Seven verification layers were bypassed not because each was weak in isolation, but because they all depended on the same static credential foundation.

Note on sources: The BleepingComputer and Taipei Times URLs listed in the source data are plausible publications for this story. URLs listed have not been independently verified by active resolution; human confirmation of source accessibility is recommended before publication. The TETRA:BURST research and prior TETRA protocol coverage referenced via industrialcyber.co and The Hacker News are corroborated by publicly documented prior reporting but those specific URL resolutions are also unconfirmed.

Action Checklist

1. Assess exposure, inventory all OT, ICS, and critical operations communication systems that use TETRA, P25, DMR, or similar radio protocols and determine when radio parameters were last rotated
2. Review credential rotation policy, verify that radio network parameters, encryption keys, and beacon credentials for any safety-critical communication system follow a documented rotation schedule enforced by policy, not assumption
3. Audit insider access to radio parameters, determine which personnel have access to TETRA or equivalent radio configuration data, apply least-privilege, and review whether insider threat controls cover operational technology environments, not just IT systems
4. Assess SDR-based monitoring gaps, evaluate whether your radio network monitoring detects unregistered transmitters or anomalous beacon sources on safety-critical frequencies; if detection capability is absent, flag as a priority gap
5. Update threat model, add low-sophistication physical-consequence attacks against OT communication infrastructure as a realistic threat scenario; TETRA:BURST (2023) established the protocol surface; this incident demonstrates that consumer hardware and static credentials are sufficient for operational disruption
6. Brief leadership and operations teams, communicate that the THSR disruption required no malware, no remote access, and no nation-state capability; frame the risk as a configuration management failure with physical safety consequences, not a software vulnerability
7. Monitor for regulatory and standards response, track whether CISA, national rail regulators, or ETSI (TETRA's standards body) issue guidance or mandatory actions following this incident

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to OT security leadership and safety operations management if: any TETRA base station CDR shows an emergency beacon activation from an unregistered ISSI, any TETRA parameter rotation date is confirmed as greater than 24 months ago on a safety-critical network, or if a physical safety event (unexpected emergency braking, train stop, signal failure) occurs within temporal proximity to anomalous RF activity on TETRA frequencies.
Recovery Notes	Following TETRA parameter rotation, verify that all authorized mobile subscriber units (train-borne radios, dispatcher handsets, maintenance terminals) have successfully re-registered with new credentials before returning any safety-critical system to full operational status — a botched rotation that locks out legitimate units is itself a safety incident. Monitor TETRA base station CDRs continuously for 30 days post-rotation for any transmissions using the old, now-invalid ISSI/GSSI values, which would indicate either a missed device or an attacker who captured and is replaying the pre-rotation parameters. Validate that the spoofed emergency beacon scenario is now operationally inert by conducting a controlled tabletop test (not a live RF test) confirming that unregistered ISSIs cannot trigger automatic safety responses.
Forensic Artifacts	TETRA base station controller Call Detail Records (CDRs): the THSR attacker's spoofed emergency beacon would appear as an SDS or status message PDU from an ISSI not present in the authorized subscriber database — pull CDRs from the 48-minute disruption window and filter for emergency PDU types (0x82, status code 32768 or equivalent emergency flag) originating from unregistered ISSIs | TETRA infrastructure management system key provisioning log: export the complete key change history for all Authentication Keys (K), Static Cipher Keys (SCK), and air interface encryption keys — the absence of any rotation events since initial deployment (circa 2006 for a THSR-pattern system) is itself primary forensic evidence of the configuration management failure that enabled the attack | RF spectrum recordings (I/Q capture): if an RTL-SDR, HackRF, or spectrum analyzer was operating on the TETRA band (380–400 MHz) during the incident window, preserve the raw I/Q recording — the attacker's consumer-grade hardware (RTL-SDR, HackRF, or similar) produces a distinct modulation quality and timing signature compared to professional TETRA infrastructure, potentially allowing physical location triangulation | Physical access logs for radio equipment rooms and tower sites: the attacker required proximity to the TETRA coverage area; combine facility access card logs (doors to equipment rooms, trackside enclosures) with the RF transmission timestamp to narrow the physical origin — an outsider with no facility access who nonetheless transmitted on-frequency confirms an external proximity attack consistent with the THSR student scenario | TETRA mobile subscriber unit registration logs: each authorized train-borne or handheld radio generates a registration event when it attaches to the network; a rogue transmitter using spoofed credentials may produce a duplicate ISSI registration collision event in the infrastructure logs, which is a specific artifact of the TETRA:BURST credential-cloning technique documented by Midnight Blue in 2023

Per-Action IR Details

Assess exposure — inventory all OT, ICS, and critical operations communication systems that use TETRA, P25, DMR, or similar radio protocols and determine when radio parameters were last rotated

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability through asset awareness and configuration baselines

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires knowing what assets exist before incidents occur, NIST SI-2 (Flaw Remediation) — static, never-rotated TETRA parameters constitute an unmitigated configuration flaw analogous to an unpatched vulnerability, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — radio communication systems including TETRA base stations, mobile subscriber units, and infrastructure controllers must be enumerated with configuration dates, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — TETRA:BURST (2023) placed TETRA radio protocol implementations on the vulnerability surface; assess whether your inventory was updated at that time

Compensating: Export your CMDB or asset tracking spreadsheet and filter for any radio, push-to-talk, or narrowband communication system. For each entry, query the system vendor's management console (e.g., Motorola MN Console, Sepura SC21, Airbus NEBULA) for the last key/parameter change timestamp. If no management console exists, contact the radio network administrator directly and require written confirmation of the last rotation date. Document all 'unknown' or 'never' responses as critical gaps.

Evidence: Before inventorying, preserve the current state: export the TETRA infrastructure controller configuration file (typically XML or proprietary binary from the base station management system) with a hash to establish a forensic baseline showing parameter age. Capture the system uptime log from each TETRA base station controller to independently corroborate claimed rotation dates — a base station online continuously since 2006 with no configuration change events is itself evidence of 19-year parameter stagnation.

Review credential rotation policy — verify that radio network parameters, encryption keys, and beacon credentials for any safety-critical communication system follow a documented rotation schedule enforced by policy, not assumption

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Policy and procedure gaps that enabled the THSR incident are a preparedness failure, not an operational one

Controls: NIST IR-8 (Incident Response Plan) — the absence of a documented TETRA key rotation schedule is an IR plan gap; the THSR attacker succeeded because no policy forced credential hygiene over 19 years, NIST IA-5 (Authenticator Management) — TETRA radio parameters, including the Authentication Key (K), Derived Cipher Key (DCK), and static emergency beacon identifiers, are authenticators subject to the same lifecycle management requirements as passwords and certificates, NIST SI-2 (Flaw Remediation) — TETRA:BURST (2023) publicly documented the exploitability of static TETRA credentials; failure to rotate after public disclosure is a flaw remediation failure, CIS 5.2 (Use Unique Passwords) — by extension, radio credentials must not be shared across base station zones or remain at vendor-default values, CIS 7.2 (Establish and Maintain a Remediation Process) — document a risk-based rotation schedule: emergency beacon parameters quarterly, encryption keys annually at minimum, consistent with ETSI EN 300 392 key management recommendations

Compensating: Create a one-page policy document that defines rotation intervals for: (1) TETRA Authentication Key (K), (2) Static Cipher Key (SCK), (3) emergency beacon identifiers (ISSI/GSSI values), and (4) air interface encryption keys (TEA1/TEA2/TEA3). Assign a named owner responsible for each rotation event. Store the policy in version control (git) alongside a rotation log CSV with columns: parameter_type, rotation_date, rotated_by, next_due_date. Set a calendar reminder 30 days before each due date.

Evidence: Preserve the current TETRA key management audit trail — most TETRA infrastructure management systems log key provisioning events to a local database or syslog. On Motorola DIMETRA or Airbus TETRA systems, export the key management log before any rotation occurs to document the gap period. If the management system has no key change records spanning years, that absence of records is itself critical forensic evidence confirming the THSR-pattern failure.

Audit insider access to radio parameters — determine which personnel have access to TETRA or equivalent radio configuration data, apply least-privilege, and review whether insider threat controls cover operational technology environments, not just IT systems

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Insider threat controls and access management are preparedness functions that reduce attack surface before incidents occur

Controls: NIST AC-6 (Least Privilege) — access to TETRA base station management consoles, key loading devices (KVL/KFD), and radio programming software (e.g., Motorola CPS, Sepura SDS) must be restricted to named personnel with a documented operational need, NIST IR-4 (Incident Handling) — the THSR attack succeeded with parameters that were presumably accessible to internal radio technicians; insider access scope defines the blast radius of parameter exfiltration, NIST AU-2 (Event Logging) — TETRA management system logins, configuration exports, and key loading events must be logged; verify that OT management consoles generate audit events and that those events are retained, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — radio network administrator accounts on TETRA infrastructure management systems must be separate from general IT accounts and require dedicated credentials, CIS 6.2 (Establish an Access Revoking Process) — verify that departed contractors or technicians who had access to TETRA configuration data have been fully deprovisioned, including physical key loading device access

Compensating: Pull the current user account list from your TETRA infrastructure management system (Motorola DIMETRA Network Manager, Airbus NEBULA, or equivalent) and cross-reference against current HR roster. Flag any accounts belonging to former employees, contractors, or vendors without active support agreements. For key loading devices (KVL/KFD hardware), maintain a physical sign-out log if no electronic audit trail exists. Review the last 90 days of management console login records manually if no SIEM is available.

Evidence: Before modifying any access, export the current access control list (ACL) and last-login timestamps from the TETRA management system as a forensic snapshot. If the THSR incident prompts an internal review, the pre-remediation access list documents who could have exfiltrated parameters and when. Also capture any key loading device (KVL) transaction logs, which record which radio units received which key versions — these establish whether parameter values were ever programmed differently across the 19-year window.

Assess SDR-based monitoring gaps — evaluate whether your radio network monitoring detects unregistered transmitters or anomalous beacon sources on safety-critical frequencies; if detection capability is absent, flag as a priority gap

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring capability must extend to the radio frequency domain for TETRA-dependent OT environments; absence of RF monitoring is a detection gap equivalent to having no network IDS

Controls: NIST SI-4 (System Monitoring) — monitoring must cover the TETRA air interface (380–400 MHz critical infrastructure band) for unauthorized transmitters; the THSR attacker's spoofed emergency beacon would have appeared as an anomalous ISSI on the network, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — TETRA infrastructure logs must be actively reviewed for unregistered ISSI/GSSI values triggering emergency procedures, not only retained, CIS 8.2 (Collect Audit Logs) — TETRA base station controllers generate call logs and registration records; these must be collected and monitored for anomalous emergency beacon activations from unregistered subscriber identities, NIST IR-5 (Incident Monitoring) — track and document any prior instances of unexpected emergency stop activations or unregistered TETRA transmitter detections as potential precursor events

Compensating: Deploy an RTL-SDR v3 or HackRF One (under $50–$300) running GNU Radio or SDR# in passive monitoring mode on the TETRA operating frequency band (380–400 MHz for European/Asian deployments). Use gr-osmocom with a TETRA demodulator plugin (e.g., osmo-tetra) to log all observed ISSI/GSSI values and compare against the authorized subscriber list. Script a Python watchdog that alerts (email or SMS via curl) when any ISSI not in the whitelist file transmits an SDS-type emergency beacon (PDU type 0x82). This is achievable by a 2-person team with open-source tooling at near-zero cost.

Evidence: If an anomalous emergency stop event has already occurred, capture: (1) TETRA base station controller call detail records (CDRs) showing the timestamp, ISSI, GSSI, and PDU type of the triggering transmission; (2) any RF spectrum analyzer logs or SDR recordings from the time window; (3) adjacent base station registration logs to determine if the rogue transmitter registered on multiple sites (indicating mobility vs. fixed position). The THSR attacker used consumer SDR hardware that would produce a distinct signal quality signature — capture I/Q recordings if available before they are overwritten.

Update threat model — add low-sophistication physical-consequence attacks against OT communication infrastructure as a realistic threat scenario; TETRA:BURST (2023) established the protocol surface; this incident demonstrates that consumer hardware and static credentials are sufficient for operational disruption

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Threat modeling is a preparedness activity; the THSR incident requires updating assumptions about adversary capability thresholds for OT communication attacks

Controls: NIST RA-3 (Risk Assessment) — the THSR incident lowers the capability threshold for TETRA-based disruption to consumer hardware ($200 SDR + publicly available TETRA:BURST tooling); prior risk assessments that assumed nation-state-level capability are now outdated and must be revised, NIST IR-4 (Incident Handling) — incident handling plans must account for scenarios where no malware, no network intrusion, and no remote access are involved; the THSR attack vector (RF spoofing) bypasses all IT-centric detection controls, NIST SI-5 (Security Alerts, Advisories, and Directives) — TETRA:BURST (2023) was a published advisory from Midnight Blue researchers; verify that your organization formally processed that advisory against OT communication assets at the time, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — extend vulnerability management scope explicitly to radio protocol implementations; TETRA, P25, and DMR are in scope for CVE/advisory monitoring just as software packages are

Compensating: Update your threat model document (or create a one-page threat scenario card) using the MITRE ATT&CK for ICS framework. Map the THSR attack to: T0855 (Unauthorized Command Message) for the spoofed emergency stop beacon, and T0868 (Detect Operating Mode) for the attacker's reconnaissance of TETRA parameters. Add a scenario card: 'Adversary with RTL-SDR and TETRA:BURST toolset transmits forged emergency beacon using static, unrotated ISSI credentials, triggering automatic safety braking on rail/transit vehicles.' No specialized tools required beyond a text editor and the ATT&CK for ICS navigator (free, browser-based).

Evidence: Pull any prior incident tickets, safety event logs, or anomaly reports involving unexpected emergency stop activations, communication interference, or unregistered radio activity on your TETRA network. These historical records may reveal undetected prior reconnaissance or test transmissions by the same or similar actors — the THSR attacker's 48-minute disruption was likely not the first transmission attempt.

Brief leadership and operations teams — communicate that the THSR disruption required no malware, no remote access, and no nation-state capability; frame the risk as a configuration management failure with physical safety consequences, not a software vulnerability

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons-learned communication and organizational awareness are explicit post-incident responsibilities; the THSR incident is an external reference event requiring internal briefing even if your organization was not directly affected

Controls: NIST IR-6 (Incident Reporting) — while this is an external incident, internal reporting obligations include briefing leadership when an industry incident reveals a directly applicable configuration risk in your own environment, NIST IR-2 (Incident Response Training) — operations and OT teams must understand that safety-critical radio communication systems are now a confirmed attack surface requiring the same credential hygiene as IT systems, NIST IR-8 (Incident Response Plan) — update the IR plan to include radio frequency spoofing as a named incident type with a defined response procedure; the THSR incident proves the scenario is no longer theoretical, CIS 7.2 (Establish and Maintain a Remediation Process) — the briefing must produce a documented remediation commitment with timelines for parameter rotation, not just awareness

Compensating: Prepare a one-page executive brief using the following structure: (1) What happened at THSR — 4 trains halted 48 minutes, consumer SDR hardware, no hacking required; (2) Why it worked — 19-year-old static TETRA parameters, equivalent to never changing a default password; (3) Our exposure — list your TETRA/P25/DMR assets and last known rotation dates; (4) Required action — specific rotation tasks with named owners and deadlines. Deliver verbally with the written brief as a leave-behind. For operations teams, use a tabletop walkthrough: 'If someone transmitted a fake emergency beacon on our TETRA frequency today, what would happen and who would know?'

Evidence: Document the briefing itself as an IR record: capture attendance, date, key decisions made, and any remediation commitments with deadlines. If leadership declines to act after a documented briefing about a publicly demonstrated, directly applicable threat, that decision and its rationale must be recorded — this creates an

accountability trail relevant to any future regulatory inquiry following an actual incident.

Monitor for regulatory and standards response — track whether CISA, national rail regulators, or ETSI (TETRA's standards body) issue guidance or mandatory actions following this incident

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Intelligence sharing and external guidance monitoring are post-incident functions that feed back into the preparation phase

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — CISA, ETSI, and national rail safety authorities are designated external organizations whose TETRA-related advisories must be received, assessed, and acted on within defined timeframes, NIST IR-8 (Incident Response Plan) — regulatory guidance following the THSR incident may impose mandatory rotation schedules or TETRA configuration standards; the IR plan must define who monitors for and processes such directives, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — track and document all regulatory communications, advisory receipts, and compliance responses as an auditable record, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the vulnerability management process must include a feed for protocol-level advisories from ETSI, CISA ICS-CERT, and sector-specific regulators (TSA for US rail, ORR for UK rail, equivalent national bodies)

Compensating: Subscribe to: (1) CISA ICS-CERT alerts at cisa.gov/ics — free email subscription, covers OT/ICS including rail; (2) ETSI publications portal for TETRA standards updates (etsi.org/standards — free registration); (3) Your national rail regulator's safety bulletin feed. Create a shared tracking document (spreadsheet or git-tracked markdown) with columns: source, advisory_date, advisory_title, applicability_to_our_environment, required_action, due_date, completed_date. Assign one team member to review this document weekly and update status. No SIEM required — this is a human process with a documented artifact.

Evidence: Maintain a dated log of all advisory receipts and your organization's formal response to each. If CISA or ETSI issues a directive following the THSR incident and your organization cannot demonstrate it was received, assessed, and either acted upon or formally risk-accepted, that gap becomes a compliance finding. The log itself — including 'no relevant guidance issued this week' entries — is the evidence of a functioning monitoring process.

Detection Guidance

Detection for this attack class is primarily at the radio network and OT monitoring layer, not the IT security stack. Key areas to audit and monitor:

Radio network anomalies: Look for beacon transmissions originating from unregistered or unexpected transmitter IDs on TETRA or equivalent safety-critical radio networks. A legitimate General Alarm or emergency beacon should originate from a known, registered device. Unregistered transmitter activity on emergency frequencies is a high-fidelity indicator of spoofing.

Unusual safety system triggers: Correlate automatic emergency braking or safety interlock activations against expected operational events. Unexplained or geographically inconsistent safety triggers, particularly affecting multiple assets simultaneously, warrant investigation of the radio communication that preceded them.

SDR hardware presence: In insider threat contexts, watch for procurement or physical presence of consumer SDR hardware (RTL-SDR, HackRF, ADALM-Pluto, and similar devices) in or near operational facilities. These are not inherently malicious but represent a low-cost capability for radio interception and transmission.

Configuration data access logs: Review access logs for TETRA radio configuration repositories, parameter stores, and encryption key management systems. The THSR attacker received parameters from an insider; detecting that exfiltration requires logging and alerting on access to radio configuration data, which many OT environments do not monitor.

TETRA:BURST indicators: Organizations referencing the 2023 TETRA:BURST research (presented Black Hat USA 2023 by Midnight Blue) should consult the disclosure documentation for protocol-level indicators relevant to their specific TETRA implementation and hardware vendor.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Consumer-grade SDR hardware (generic class: RTL-SDR, HackRF, or equivalent)`	SDR hardware leveraged via physical proximity to TETRA radio network to intercept static radio parameters and transmit a forged General Alarm emergency beacon, triggering automatic emergency braking on four THSR trains	HIGH
TOOL	`TETRA radio parameter set (static, unrotated — 19 years)`	Static TETRA network credentials intercepted and reused to impersonate a legitimate emergency beacon; parameters had not been rotated since THSR network deployment, allowing credential reuse without cryptographic attack	HIGH
URL	`Pending — refer to BleepingComputer (bleepingcomputer.com) and Taipei Times (taipeitimes.com) for published incident indicators if available`	Source articles for the April 5, 2026 THSR incident; URLs listed in item data were not actively resolved and should be treated as unverified pending human confirmation — no specific IOC values extracted	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1040** — Network Sniffing
- **T1499.004** — Application or System Exploitation
- **T1200** — Hardware Additions
- **T0803** — Block Command Message
- **T1562.001** — Disable or Modify Tools
- **T1602** — Data from Configuration Repository
- **T0855** — Unauthorized Command Message

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)

- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

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

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

HIPAA-SECURITY

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1040	Network Sniffing	Credential-Access
T1499.004	Application or System Exploitation	Impact
T1200	Hardware Additions	Initial-Access
T0803	Block Command Message	Inhibit-Response-Function

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1602	Data from Configuration Repository	Collection
T0855	Unauthorized Command Message	Impair-Process-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/student-hacked-taiwa...	T3
Student's hack prompts THSRC review - Taipei Times	https://www.taipeitimes.com/News/taiwan/archives/2026/05/05/2003856781	T3
Multiple flaws found in TETRA radio systems, exposing law ...	https://industrialcyber.co/threats-attacks/multiple-flaws-found-in-...	T3
New TETRA Radio Encryption Flaws Expose Law Enforcement ...	https://thehackernews.com/2025/08/new-tetra-radio-encryption-flaws-...	T3
Addressing the TETRA System Backdoor Challenge Through ...	https://www.preprints.org/manuscript/202408.1728	T3

Generated 2026-05-06 08:40 UTC by TJS Security Command Center