INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-15 13:51 UTC

# SDR-Based RF Disruption of Taiwanese High-Speed Rail Exposes OT Signaling Vulnerabilities

SECURITY ANALYSIS | HIGH | CVSS 7.5

| | |
|---|---|
| SCC Item ID | SCC-STY-2026-0131 |
| Type | Security Analysis |
| Severity | HIGH |
| CVSS Base Score | 7.5 |
| Affected Products | Taiwan High-Speed Rail Corporation (THSRC) train control and signaling systems, vendor and specific system versions not publicly disclosed |
| Published | 2026-05-14T21:00:00 |
| Discovery Source | Rss |

## Executive Summary

A Taiwanese university student disrupted three high-speed rail services for approximately one hour using low-cost software-defined radio equipment, exploiting unauthenticated RF-based signaling protocols, including a system that had not rotated cryptographic keys in 19 years. The incident demonstrates that legacy OT environments in critical transportation infrastructure present a measurable, low-barrier attack surface that does not require nation-state resources or insider access. For security leaders, this is a signal: the same RF authentication gaps exist across rail, transit, and industrial control environments globally, and the cost of basic RF injection equipment has fallen to commodity hardware, creating a measurable barrier-to-entry reduction for adversaries with technical knowledge and physical proximity to the target infrastructure.

## Technical Analysis

The attacker, a university student in Taiwan, used software-defined radio (SDR) hardware, widely available for under $50 USD, to inject or interfere with RF-based control and signaling traffic on Taiwan High Speed Rail Corporation (THSRC) infrastructure. The disruption halted or delayed three train services for roughly one hour and triggered an anti-terrorism response, indicating the severity of the operational impact was immediately recognized by authorities.

The attack exploited three compounding weaknesses. First, the RF control protocol lacked cryptographic authentication (CWE-287), meaning the signaling channel accepted commands or interference without verifying origin. Second, the system performed no origin validation on received RF signals (CWE-346), leaving it unable to distinguish legitimate control messages from injected ones. Third, there was no interference detection or protection mechanism in place (CWE-693) to alert operators or fail safely when anomalous RF activity was present. Reporting from Tom's Hardware and Security Affairs indicates the underlying system had not rotated cryptographic keys in 19 years, a detail that, if accurate, suggests the vulnerability was not the result of a single missed patch cycle but of systemic neglect of OT security lifecycle management.

MITRE ATT&CK for ICS maps this incident across several relevant techniques: T0800 (Activate Firmware Update Mode), T0830 (Adversary-in-the-Middle), T0816 (Device Restart/Shutdown), and T0831 (Manipulation of Control), along with T1498 (Network Denial of Service) in the sense of service disruption, and T1195 (Supply Chain Compromise) as a generalized risk context for the vendor ecosystem. The most operationally relevant techniques here are T0830 and T0831, the attacker positioned SDR equipment to influence or override control signals, achieving physical-world impact without network access.

No CVE has been assigned because this is a protocol-level architectural flaw (unauthenticated RF signaling) rather than a discrete software vulnerability, making it outside the scope of CVE assignment criteria. The applicable CWEs (CWE-287, CWE-346, CWE-693) describe architectural deficiencies rather than patchable code flaws, which makes remediation a longer-cycle engineering problem requiring system redesign rather than a patch deployment. CVSS scoring does not apply; qualitative severity (High) is assigned editorially based on the confirmed operational impact (three-train disruption), low barrier to entry, and applicability to critical infrastructure globally.

The broader industry implication is significant. Rail signaling systems in multiple countries, particularly those built or last upgraded before 2010, may rely on similar unauthenticated RF protocols. The THSRC incident is notable precisely because the attacker required no insider knowledge, no network access, and no sophisticated tooling. The attack surface is physical proximity plus commodity hardware, a threat model that OT security programs designed around network-layer controls are not built to address.

## Action Checklist

1. Step 1: Assess OT RF exposure, inventory all radio frequency-based control, signaling, or telemetry systems in your OT environment; determine whether they use authenticated protocols or legacy unauthenticated RF standards
2. Step 2: Review cryptographic hygiene on OT systems, audit key rotation schedules for any OT control system using cryptographic authentication; flag systems where keys have not been rotated in more than 3 years for immediate review
3. Step 3: Evaluate physical proximity threat model, assess whether adversaries with SDR equipment (low-cost, widely available) could reach operational range of your RF-dependent OT systems from public or semi-public space
4. Step 4: Review detection capability gaps, determine whether your OT monitoring stack includes RF-layer anomaly detection capability (e.g., spectrum monitoring, RF IDS). Note that traditional network-layer OT monitoring tools (Claroty, Dragos, Nozomi) do not natively detect RF-layer attacks; RF detection requires dedicated spectrum monitoring or RF intrusion detection systems deployed separately
5. Step 5: Update threat model, add low-sophistication physical-layer RF interference as a credible threat vector in your OT risk register, not only nation-state actors; the THSRC incident establishes that the barrier

to entry is low

6. Step 6: Communicate findings to operations leadership, brief rail, transit, utilities, or industrial operations leads on the THSRC incident as a concrete risk case; avoid framing this as a theoretical concern given confirmed real-world impact

7. Step 7: Monitor THSRC security review disclosures and CISA ICS advisories, track for follow-up technical guidance from CISA ICS-CERT or sector-specific ISACs (e.g., IT-ISAC, surface transportation ISAC) that may issue guidance in response to this incident

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | URGENT |
| **Escalation Criteria** | Escalate immediately to OT operations leadership and CISA (via cisa.gov/report) if any of the following are confirmed: (1) unexpected RF signal activity observed on OT signaling frequencies during operational hours; (2) unexplained train control system commands, service disruptions, or signaling anomalies coinciding with RF spectrum activity; (3) discovery that any deployed OT RF signaling system uses unauthenticated protocols or has not undergone key rotation in more than 3 years and is reachable from public space — each of these conditions individually meets the threshold for escalation given the THSRC incident's confirmation that exploitation is achievable with commodity equipment. |
| **Recovery Notes** | Following any confirmed or suspected RF disruption event, do not restore OT signaling systems to normal operations until the RF environment on all operational frequencies has been verified clean using SDR spectrum monitoring from multiple physical vantage points, and any anomalous transmission sources have been located and neutralized or attributed. Engage OT system vendors to perform a post-incident cryptographic key rotation on all affected RF signaling systems before returning them to service, treating unrotated keys as compromised if the attacker had sufficient dwell time to capture and analyze RF transmissions. Maintain continuous RF spectrum monitoring for a minimum of 30 days post-recovery to detect recurrence or reconnaissance activity, and preserve all SDR logs and OT historian data from the incident window as forensic evidence. |

| | |
|---|---|
| **Forensic Artifacts** | SDR spectrum recordings (IQ sample files in .wav or .sigmf format) captured at the time of the disruption event, covering the operational RF frequencies of the affected signaling system — these recordings may contain the injected or jamming signal and can be analyzed offline using GNU Radio or Universal Radio Hacker (URH) to characterize the attack waveform and transmission source \| OT historian or SCADA event logs from the train control system recording unexpected command states, signal drops, or ATC system faults during the disruption window — for rail systems, this includes Automatic Train Protection (ATP) and Automatic Train Control (ATC) event logs with millisecond-resolution timestamps that can be correlated against the RF activity timeline \| Physical security camera footage from station platforms, perimeter areas, and any public vantage points within RF range of the signaling system during the disruption window — the THSRC attacker operated from a physically accessible location, making CCTV footage a primary artifact for identifying the threat actor and their equipment \| RF signal strength and frequency logs from any installed spectrum monitoring equipment or from the OT vendor's diagnostic interface, showing anomalous signal presence or RSSI spikes on signaling frequencies that do not correspond to scheduled train movements or legitimate control system transmissions \| Vendor maintenance and key provisioning records for the affected signaling system, including the cryptographic key version, provisioning date, and last rotation event — in the THSRC case, a 19-year absence of key rotation records is itself a forensic artifact establishing the vulnerability condition and is required for regulatory disclosure and post-incident reporting |

## Per-Action IR Details

### Step 1: Assess OT RF exposure — inventory all radio frequency-based control, signaling, or telemetry systems in your OT environment; determine whether they use authenticated protocols or legacy unauthenticated RF standards

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Establishing IR capability through asset visibility and threat surface enumeration

**Controls:** NIST IR-4 (Incident Handling) — preparation component requires knowing which systems are in scope, NIST SI-4 (System Monitoring) — monitoring scope must include RF-layer telemetry and control channels, not only IP network interfaces, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — inventory must extend to OT RF-dependent assets including train control transponders, ATC balise readers, TETRA/GSM-R radio systems, and any legacy proprietary RF signaling equipment, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — RF protocol authentication status must be a documented attribute in the vulnerability management scope

**Compensating:** Use a calibrated SDR receiver (RTL-SDR V3, ~$25) with GNU Radio or GQRX to passively scan the 400–900 MHz and 2.4 GHz bands from within your OT perimeter and note all active transmissions; cross-reference observed frequencies against your asset list. For each unidentified signal, use a spectrum analyzer log export and match against known rail/transit protocol bands (e.g., 450 MHz ATC, 900 MHz SCADA telemetry). Document protocol, authentication method, and last key rotation date in a spreadsheet — a 2-person team can complete a facility sweep in one working day.

**Evidence:** Before inventorying, capture a passive RF spectrum baseline using SDR equipment at multiple physical vantage points within the OT facility perimeter; log center frequencies, signal strength, modulation type, and transmission intervals for all observed signals. Retain this baseline as forensic reference for future anomaly detection. Also collect existing asset documentation: vendor datasheets for installed signaling equipment, purchase order records showing procurement dates (to establish protocol vintage), and any network architecture diagrams that reference RF interfaces.

### Step 2: Review cryptographic hygiene on OT systems — audit key rotation schedules for any OT control system using cryptographic authentication; flag systems where keys have not been rotated in more than 3 years for immediate review

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Identifying and remediating conditions that would degrade IR effectiveness or enable exploitation

**Controls:** NIST SI-2 (Flaw Remediation) — cryptographic key exhaustion and protocol obsolescence in OT signaling systems constitute remediable flaws; 19-year key non-rotation as observed in the THSRC incident is a documented failure mode, NIST SI-7 (Software, Firmware, and Information Integrity) — integrity of OT control commands depends on valid cryptographic authentication; stale or absent keys undermine this control entirely, NIST IR-8 (Incident Response Plan) — IR plan must document the specific response procedure if a key compromise is suspected in an OT RF signaling context, where re-keying may require physical access and scheduled maintenance windows, CIS 4.6 (Securely Manage Enterprise Assets and Software) — key material and cryptographic configuration for OT RF systems must be managed under the same configuration governance as software; undocumented 19-year-old keys represent a configuration management failure

**Compensating:** Request key provisioning records from OT system vendors for all RF-authenticated signaling equipment; if records are unavailable, treat the system as having unknown key age. For systems that support it, use vendor diagnostic tools or serial console access to query current key version and last-modified timestamp. Document findings in a simple CSV: system name, protocol, key type, provisioning date, last rotation date, rotation authority. Flag any system with no documented rotation event within 36 months for escalation to the OT system vendor.

**Evidence:** Collect vendor maintenance logs and any historian records that capture configuration change events for OT signaling systems — specifically look for entries corresponding to key provisioning or cryptographic parameter updates. For rail systems, request maintenance work order history from the operations team: a 19-year absence of key rotation entries (as in the THSRC incident) is itself a forensic artifact demonstrating the vulnerability condition. Preserve these records before initiating any remediation, as they establish the pre-incident configuration state for post-incident review.

### Step 3: Evaluate physical proximity threat model — assess whether adversaries with SDR equipment (low-cost, widely available) could reach operational range of your RF-dependent OT systems from public or semi-public space

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Threat modeling and attack surface assessment prior to incident occurrence

**Controls:** NIST RA-3 (Risk Assessment) — the THSRC incident establishes that SDR-based RF disruption of rail signaling is not a theoretical risk; a university student with commodity equipment disrupted three services, which must now be treated as a baseline threat scenario in OT rail/transit risk assessments, NIST IR-4 (Incident Handling) — incident handling preparation for RF-based disruption must account for the attacker's ability to operate from public space (station platforms, adjacent roads, parking areas) without requiring physical access to secure zones, CIS 4.4 (Implement and Manage a Firewall on Servers) — physical RF boundary analogous to network perimeter: assess whether existing physical security controls (fencing, standoff distance, RF shielding) actually prevent an SDR operator from achieving effective range on operational frequencies, CIS 4.5 (Implement and Manage a Firewall on End-User Devices) — by analogy, RF-layer isolation must be evaluated as a perimeter control; identify whether any RF signaling interface is reachable from outside the physical security boundary

**Compensating:** Conduct a walk-test using an RTL-SDR receiver to physically verify at what distance and from which public vantage points (station platforms, roadways, parking areas) your OT RF signals are receivable and at what signal strength. Map these locations against your physical security perimeter. Use Google Maps or OpenStreetMap to document standoff distances and identify uncontrolled public spaces within range. This produces a proximity threat map that a 2-person team can generate in a half-day site survey without specialized equipment beyond a laptop and SDR dongle.

**Evidence:** Before conducting the proximity assessment, document the current physical security boundary (fencing extent, camera coverage, guard patrol routes) using facility maps and physical security records. Capture SDR signal reception logs during the walk-test, recording GPS coordinates (or measured distances) and received signal strength indicator (RSSI) values at each vantage point. These logs establish the physical attack surface baseline and serve as evidence of the pre-remediation exposure condition.

**Step 4: Review detection capability gaps — determine whether your OT monitoring stack (e.g., Claroty, Dragos, Nozomi) includes RF anomaly detection or whether you rely solely on network-layer visibility; note the gap if RF-layer monitoring is absent**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: Identifying gaps in monitoring coverage that would prevent detection of the THSRC-style RF disruption attack vector

**Controls:** NIST SI-4 (System Monitoring) — network-layer OT monitoring tools (Claroty, Dragos, Nozomi) operate on Ethernet/IP traffic and do not observe RF-layer signaling; the THSRC attack occurred entirely at the RF physical layer and would not generate alerts in any of these platforms, NIST AU-2 (Event Logging) — RF-layer events (unexpected frequency activity, signal strength anomalies, jamming signatures) are not logged by standard OT monitoring stacks; this represents an AU-2 gap specific to the RF attack surface exposed by the THSRC incident, NIST IR-5 (Incident Monitoring) — incident monitoring scope must be expanded to include RF-layer anomaly detection for OT environments with radio-dependent signaling, CIS 8.2 (Collect Audit Logs) — audit log collection must include RF monitoring data sources; if RF-layer logs do not exist, document this as a capability gap with a remediation timeline

**Compensating:** Deploy an RTL-SDR receiver connected to a Raspberry Pi running rtl_power or gr-scan to continuously log signal activity on known OT RF frequencies; configure alerting via a simple Python script that triggers on unexpected signal presence or RSSI spikes during non-operational hours. For a budget solution, use GQRX with a scheduled recording job and daily manual review of spectrum waterfall logs. This provides passive RF anomaly detection without commercial tooling and is operable by a 2-person team with basic Linux skills.

**Evidence:** Query your existing OT monitoring platform (Claroty, Dragos, or Nozomi) for any alerts or telemetry corresponding to the time window of any known operational disruption — note that for an RF-layer attack identical to THSRC, these platforms will show no alerts, which is itself forensic evidence of the detection gap. Collect the platform's asset coverage report to document which OT assets are monitored and confirm that none include RF interface visibility. Preserve these reports as pre-remediation baseline documentation.

**Step 5: Update threat model — add low-sophistication physical-layer RF interference as a credible threat vector in your OT risk register, not only nation-state actors; the THSRC incident establishes that the barrier to entry is low**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Threat intelligence integration into IR readiness and risk posture

**Controls:** NIST RA-3 (Risk Assessment) — the THSRC incident is a confirmed real-world precedent that SDR-based RF disruption of high-speed rail signaling is achievable by a non-state actor with commodity equipment costing under $200; this must be reflected in the likelihood scoring of physical RF threats in OT risk registers, NIST IR-8 (Incident Response Plan) — the IR plan must include a scenario for RF-layer disruption of OT signaling that does not assume sophisticated attacker resources, insider access, or network-layer compromise, NIST SI-5 (Security Alerts, Advisories, and Directives) — the THSRC incident constitutes a security advisory event; organizations in rail, transit, utilities, and industrial sectors should treat it as a trigger to update threat assumptions, CIS 7.2 (Establish and Maintain a Remediation Process) — the risk register update must include a remediation priority and timeline for RF authentication gaps, not merely a documentation entry

**Compensating:** Use the MITRE ATT&CK for ICS framework (specifically T0816 — Device Restart/Shutdown and T0828 — Loss of Safety) as structured vocabulary to document the THSRC-style threat scenario in your risk register without requiring a commercial GRC platform. A simple spreadsheet risk register entry should include: threat actor profile (low-sophistication, physical proximity), attack vector (SDR RF injection/jamming), affected asset class (unauthenticated RF signaling systems), likelihood (confirmed real-world precedent), and impact (service disruption, potential safety event). Update this entry quarterly as CISA ICS advisories are released.

**Evidence:** Before updating the threat model, retrieve and preserve the current version of your OT risk register to establish a documented baseline of the pre-update threat assumptions. Archive any prior risk assessment reports that classified RF-layer threats as theoretical or nation-state-only — these records demonstrate the pre-THSRC risk posture and will be relevant in post-incident reviews or regulatory inquiries if an RF-based incident subsequently occurs.

**Step 6: Communicate findings to operations leadership — brief rail, transit, utilities, or industrial operations leads on the THSRC incident as a concrete risk case; avoid framing this as a theoretical concern given confirmed real-world impact**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned dissemination and organizational risk communication based on external incident precedent

**Controls:** NIST IR-6 (Incident Reporting) — while the THSRC incident is external, IR-6 reporting obligations extend to informing internal stakeholders of credible threats; operations leadership responsible for rail or OT environments must be briefed on confirmed RF disruption capability, NIST IR-2 (Incident Response Training) — the THSRC incident provides a concrete training scenario for operations and security teams; briefing leadership is the first step toward incorporating this scenario into tabletop exercises, NIST IR-7 (Incident Response Assistance) — leadership briefing should include escalation paths: who to call if RF disruption is suspected during operations, including OT vendor contacts and sector ISAC notification procedures, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — leadership must understand that RF authentication gaps in legacy OT signaling systems are a vulnerability class requiring the same management attention as software CVEs

**Compensating:** Prepare a one-page briefing document referencing the THSRC incident with three elements: (1) what happened — a student disrupted three high-speed rail services for one hour using a $200 SDR device by exploiting unauthenticated RF signaling including a system with 19-year-old cryptographic keys; (2) what the exposure means for your environment — list specific RF-dependent OT assets identified in Step 1; (3) what decisions are needed — budget for RF monitoring capability, vendor engagement for key rotation, or physical security enhancements. No commercial tools required; deliver via email with a meeting request.

**Evidence:** Before the briefing, compile the outputs from Steps 1–5 as supporting documentation: the RF asset inventory, cryptographic hygiene audit results, proximity threat map, detection gap assessment, and updated risk register entry. These documents transform the briefing from an anecdote into a data-supported risk case and create a paper trail demonstrating that the security team performed due diligence in response to the THSRC incident.

**Step 7: Monitor THSRC security review disclosures and CISA ICS advisories — track for follow-up technical guidance from CISA ICS-CERT or sector-specific ISACs (e.g., IT-ISAC, surface transportation ISAC) that may issue guidance in response to this incident**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Intelligence sharing and continuous improvement based on external incident disclosures

**Controls:** NIST SI-5 (Security Alerts, Advisories, and Directives) — organizations must maintain a process for receiving and acting on ICS-CERT advisories; the THSRC incident may trigger CISA guidance specific to RF-authenticated OT signaling systems in the transportation sector, NIST IR-5 (Incident Monitoring) — incident monitoring scope includes tracking external incident disclosures that affect your threat model; THSRC follow-up disclosures (e.g., vendor advisories, government investigation findings) constitute actionable intelligence, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — any new technical indicators or attack signatures published in CISA advisories or ISAC bulletins following the THSRC incident must be incorporated into OT monitoring review procedures, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the vulnerability management process must include a trigger to re-assess RF OT assets whenever CISA ICS-CERT publishes advisories referencing unauthenticated RF protocols or SDR-based attack techniques

**Compensating:** Subscribe to CISA ICS-CERT advisories via the free email notification service at cisa.gov/ics-cert; set up a Google Alert or RSS feed for 'THSRC security,' 'SDR rail signaling,' and 'OT RF vulnerability.' Monitor the Surface Transportation ISAC (ST-ISAC) and IT-ISAC member bulletins if your organization has membership; if not, the free CISA alert subscription provides the minimum viable intelligence feed. Assign one team member to review these feeds weekly and log any new guidance against the risk register entry created in Step 5.

**Evidence:** Maintain a dated log of all CISA ICS advisories, vendor security bulletins, and ISAC notifications reviewed in response to the THSRC incident; record the review date, advisory identifier, content summary, and any action taken. This log serves as evidence of continuous monitoring compliance under NIST SI-5 (Security Alerts, Advisories, and Directives) and provides an audit trail demonstrating that the organization tracked post-incident disclosures and

responded to new technical guidance as it became available.

## Detection Guidance

Detection for RF-layer OT attacks is not achievable through standard network monitoring alone. Security teams should consider the following approaches based on the THSRC attack pattern:

**RF spectrum monitoring:** Deploy spectrum analyzers or dedicated RF intrusion detection systems in proximity to critical OT signaling infrastructure. Anomalous signal activity on operational frequencies, unexpected transmissions, signal strength spikes, or protocol-inconsistent frames, should generate alerts. Note: RF anomaly detection for OT is not yet a mature, standardized product category; organizations may need to partner with RF engineering or spectrum monitoring vendors to implement this capability, or deploy general-purpose spectrum analyzers with manual alerting rules.

**OT historian and SCADA anomaly detection:** Review historian logs and SCADA event logs for unexpected control state changes, emergency braking events, or signal loss events that do not correlate with scheduled maintenance or known environmental conditions. Clustering of unexplained state changes across multiple assets in a short window (as occurred with three trains in the THSRC incident) is a behavioral indicator.

**Physical security audit:** Assess whether adversaries with handheld SDR equipment could achieve operational proximity to signaling infrastructure from publicly accessible areas, station platforms, roads adjacent to rail corridors, or parking structures. Physical access controls may need to address RF range, not only direct physical contact.

**Protocol authentication audit:** For organizations operating legacy rail or industrial RF control systems, audit whether the control protocol enforces message authentication codes (MACs) or digital signatures on command frames. The absence of authentication is not detectable in logs, it requires a protocol-layer review against the vendor's technical documentation.

**Key rotation compliance check:** Audit OT system configurations for cryptographic key age. A system with keys unchanged for years or decades is a priority finding regardless of whether active exploitation has been observed.

## Framework Mappings

### MITRE-ATTACK

- **T0800** — Activate Firmware Update Mode
- **T1195** — Supply Chain Compromise
- **T0830** — Adversary-in-the-Middle
- **T1498** — Network Denial of Service
- **T0816** — Device Restart/Shutdown
- **T0831** — Manipulation of Control

### NIST-800-53R5

- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes

- **SI-7** — Software, Firmware, and Information Integrity
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SC-13** — Cryptographic Protection
- **SI-4** — System Monitoring

**OWASP-TOP10-2021**

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

**CIS-V8**

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **8.2** — Collect Audit Logs

**SOC2-TSC**

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

**HIPAA-SECURITY**

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

**ISO-27001-2022**

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

**NIST-CSF-2**

- **DE.CM-01** — Networks and network services are monitored

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T0800 | Activate Firmware Update Mode | Inhibit-Response-Function |
| T1195 | Supply Chain Compromise | Initial-Access |
| T0830 | Adversary-in-the-Middle | Collection |
| T1498 | Network Denial of Service | Impact |
| T0816 | Device Restart/Shutdown | Inhibit-Response-Function |
| T0831 | Manipulation of Control | Impact |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.darkreading.com/ics-ot-security/taiwan-incident-highlig... | T3 |
| **Taiwan High-Speed Rail Breach Reveals Critical Infrastructure ...** | https://dominotheory.com/taiwan-high-speed-rail-breach-reveals-crit... | T3 |
| **College student hacks Taiwan high-speed rail line with software ...** | https://www.tomshardware.com/tech-industry/cyber-security/college-s... | T3 |
| **Student's hack prompts THSRC review - Taipei Times** | https://www.taipeitimes.com/News/taiwan/archives/2026/05/05/2003856781 | T3 |
| **Taiwan High-Speed Rail Emergency Braking Hack: How a Student ...** | https://securityaffairs.com/191785/hacking/taiwan-high-speed-rail-e... | T3 |



Generated 2026-05-15 13:51 UTC by TJS Security Command Center