INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-06-14 04:23 UTC

FUXA SCADA/HMI Authorization Bypass Allows Unauthenticated Scheduler Manipulation (CVE-2026-25939)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0298
Type	CVE Vulnerability
CVE ID	CVE-2026-25939
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0002 (7th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability
Affected Products	frangoteam FUXA versions 1.2.8 through 1.2.10; patched in 1.2.11
Published	2026-06-12T00:00:00Z
Discovery Source	Vulncheck Kev

Executive Summary

A critical authorization bypass vulnerability in FUXA, a web-based SCADA/HMI platform used in industrial control environments, allows unauthenticated remote attackers to create and modify operational schedulers without credentials. Versions 1.2.8 through 1.2.10 are affected; a patch is available in version 1.2.11. Organizations running FUXA in OT/ICS environments face direct risk of automated process manipulation, which could disrupt industrial operations or cause physical-world consequences.

Technical Analysis

CVE-2026-25939 is a missing authorization vulnerability (CWE-862) in frangoteam FUXA versions 1.2.8 through 1.2.10, a web-based SCADA/HMI/dashboard platform. An unauthenticated, remote attacker can reach the scheduler management API without any credential requirement, enabling arbitrary creation and modification of scheduled tasks. Because FUXA interfaces with OT systems, scheduler manipulation translates directly to influence over industrial process automation. The vulnerability maps to MITRE ATT&CK T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), and ICS-specific T0883 (Internet Accessible Device). CISA has cataloged this vulnerability in the Known Exploited Vulnerabilities catalog, indicating active exploitation. A public proof-of-concept repository

(mbanyamer/CVE-2026-25939-SCADA-FUXA-Unauthenticated-Remote-Arbitrary) is publicly available on GitHub, lowering the exploitation barrier significantly. CVSS base score is 9.8. The fix is FUXA version 1.2.11, available from the frangoteam repository.

Action Checklist

1. Step 1: Containment, Immediately isolate FUXA instances (versions 1.2.8-1.2.10) from internet-facing access. Apply network-layer controls to restrict the FUXA web interface to authorized internal hosts only. If internet exposure cannot be immediately removed, place the service behind an authenticated reverse proxy or VPN gateway. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query web server and application access logs for unauthenticated POST/PUT/PATCH requests to scheduler-related API endpoints (e.g., /api/scheduler, /scheduler, or equivalent FUXA routing paths) originating from unexpected source IPs. Flag any scheduler creation or modification events that lack a corresponding authenticated session token. Review FUXA audit logs for scheduler entries not initiated by known operator accounts. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Step 3: Eradication, Upgrade all FUXA deployments to version 1.2.11 from the official frangoteam repository. Verify the installed version post-upgrade. After patching, audit all existing scheduler configurations for unauthorized entries and remove any tasks not created by authorized operators. Rotate credentials for any accounts that may have been exposed to the FUXA interface during the vulnerable window. Reference: NIST SI-4 (System Monitoring), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), D3-CRO (Credential Rotation).
4. Step 4: Recovery, After upgrading to 1.2.11, validate that the scheduler API now enforces authentication by attempting an unauthenticated request and confirming rejection. Restore scheduler configurations from a known-good backup predating any suspected exploitation window. Re-enable OT system connectivity only after confirming scheduler integrity. Monitor FUXA application logs and connected OT telemetry for anomalous process behavior for at least 72 hours post-remediation. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), D3-LAM (Local Account Monitoring).
5. Step 5: Post-Incident, Conduct a network segmentation review to confirm FUXA and other HMI/SCADA interfaces are not directly internet-reachable. Implement a recurring review of FUXA scheduler configurations as part of OT change management. Evaluate whether authentication controls on all ICS-facing web applications meet the standard required by your OT security policy. Document lessons learned and update the ICS incident response playbook to include FUXA-specific indicators. Reference: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), D3-UAP (User Account Permissions), D3-MFA (Multi-factor Authentication).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to OT security leadership and ICS incident response if: any unauthorized FUXA scheduler entry is confirmed to have executed (correlate scheduler timestamps against OT process historian data), if FUXA is confirmed internet-exposed with evidence of external exploitation, or if regulated critical infrastructure sectors (energy, water, manufacturing) are affected — which may trigger sector-specific regulatory notification obligations (e.g., NERC CIP, EPA/CISA reporting under CIRCIA).
Recovery Notes	After upgrading to FUXA 1.2.11 and restoring a known-good scheduler configuration, validate authentication enforcement via unauthenticated API test before reconnecting any OT systems. Monitor FUXA application logs and OT process telemetry continuously for a minimum of 72 hours post-recovery, specifically watching for scheduler entries reappearing outside of authorized change windows or process behaviors deviating from pre-incident baselines. Do not restore internet-facing exposure to FUXA under any circumstances without enforced authentication (MFA-backed reverse proxy or VPN) and documented approval from OT security leadership.
Forensic Artifacts	FUXA web server access logs: HTTP method, URI path, source IP, and Authorization header presence — specifically POST/PUT/PATCH requests to /api/scheduler or equivalent routing paths with null or absent session tokens, covering the full deployment window of versions 1.2.8–1.2.10 | FUXA scheduler persistence store (schedulers.json or equivalent file in ./FUXA/store/): captures all scheduler objects written to disk, including any unauthorized tasks injected by an unauthenticated attacker, preserving task names, execution times, and associated commands or scripts | Operating system process execution logs for the FUXA host: on Linux, `/var/log/syslog` or `journalctl -u fuxa` for child process spawning triggered by scheduler execution; on Windows, Security Event Log Event ID 4688 (Process Creation) filtered on processes spawned by the FUXA Node.js parent process during the suspicious scheduler execution window | Network flow records or packet capture on the FUXA host's OT-facing interface: captures any anomalous commands or protocol messages sent to downstream SCADA/PLC devices during the window when unauthorized schedulers may have executed, enabling correlation between scheduler execution timestamps and OT process changes | FUXA user/account database and session log: documents which accounts were active, last login timestamps, and whether any session tokens were issued during the exploitation window — used to determine whether the authorization bypass was the sole attack vector or whether compromised credentials were also leveraged

Per-Action IR Details

Step 1: Containment — Immediately isolate FUXA instances (versions 1.2.8–1.2.10) from internet-facing access. Apply network-layer controls to restrict the FUXA web interface to authorized internal hosts only. If internet exposure cannot be immediately removed, place the service behind an authenticated reverse proxy or VPN gateway. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On Linux hosts: `iptables -I INPUT -p tcp --dport ! -s -j DROP` to block all non-authorized source IPs at the host firewall. On Windows: use `netsh advfirewall firewall add rule` to restrict the FUXA web port. If a reverse proxy is available, deploy Nginx with `allow ; deny all;` in the location block for FUXA routes, requiring HTTP Basic Auth or client certificate as an immediate authentication layer until VPN can be enforced.

Evidence: Before isolating the host or changing firewall rules, capture: (1) active TCP connections to the FUXA web port via `ss -tnp sport = :` or `netstat -ano | findstr ` to identify any currently active attacker sessions; (2) a full memory

dump of the FUXA process (e.g., using `procdump -ma ` on Windows or `gcore ` on Linux) to preserve in-memory scheduler state and any injected content; (3) a snapshot of the FUXA data directory and scheduler configuration files (typically under `./FUXA/store/` or equivalent) before any network change alters application state.

Step 2: Detection — Query web server and application access logs for unauthenticated POST/PUT/PATCH requests to scheduler-related API endpoints (e.g., /api/scheduler, /scheduler, or equivalent FUXA routing paths) originating from unexpected source IPs. Flag any scheduler creation or modification events that lack a corresponding authenticated session token. Review FUXA audit logs for scheduler entries not initiated by known operator accounts. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following against FUXA's Node.js/Express access log (default path varies by deployment; check `./FUXA/logs/` or the systemd journal via `journalctl -u fuxa`): `grep -E 'POST|PUT|PATCH' access.log | grep -E '/api/scheduler|/scheduler' | grep -v 'Authorization:'` to surface unauthenticated scheduler write requests. Cross-reference source IPs against known operator workstation ranges. Use `jq` to parse FUXA's structured JSON logs if available: `jq 'select(.method=="POST" and (.url | test("scheduler")) and (.headers.authorization == null))' fuxa.log`. Timestamp any matches against known operator shift schedules to identify out-of-hours activity.

Evidence: This is a read/analysis step that does not alter live state; however, preserve log files before any patch or service restart destroys them. Collect: (1) FUXA application access logs covering the full vulnerable window (versions 1.2.8–1.2.10 deployment date through isolation); (2) the FUXA scheduler store file (e.g., `schedulers.json` or equivalent persistence file in `./FUXA/store/`) to document all scheduler entries present at time of detection; (3) any FUXA audit trail entries recording scheduler create/modify events without an associated authenticated user token.

Step 3: Eradication — Upgrade all FUXA deployments to version 1.2.11 from the official frangoteam repository. Verify the installed version post-upgrade. After patching, audit all existing scheduler configurations for unauthorized entries and remove any tasks not created by authorized operators. Rotate credentials for any accounts that may have been exposed to the FUXA interface during the vulnerable window. Reference: NIST SI-4 (System Monitoring), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: 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: Download FUXA 1.2.11 directly from the official frangoteam GitHub repository (https://github.com/frangoteam/FUXA/releases — verify the release tag and SHA checksum before deploying). Stop the FUXA service (`systemctl stop fuxa` or `pm2 stop fuxa`), back up the existing `./FUXA/store/` directory, install 1.2.11, and restart. Confirm the running version via the FUXA UI About page or by inspecting `package.json` in the installation directory: `cat /opt/fuxa/package.json | grep version`. For credential rotation without an IdP, manually reset all FUXA operator account passwords via the admin interface and revoke any API tokens stored in the FUXA configuration.

Evidence: Before applying the patch or rotating credentials (both alter live state), capture: (1) a full export of the current FUXA scheduler store (`schedulers.json` or equivalent) to document all unauthorized scheduler entries for forensic record and to support legal or regulatory notification if needed; (2) running process list and active network connections at time of eradication (`ps aux | grep fuxa` and `ss -tnp`) to confirm no active attacker session persists; (3) a copy of FUXA's user/account database file to document which accounts existed and their last-login timestamps during the vulnerable window. These captures must precede the patch application and credential rotation.

Step 4: Recovery — After upgrading to 1.2.11, validate that the scheduler API now enforces authentication by attempting an unauthenticated request and confirming rejection. Restore scheduler configurations from a known-good backup predating any suspected exploitation window. Re-enable OT system connectivity only after confirming scheduler integrity. Monitor FUXA application logs and connected OT telemetry for anomalous process behavior for at least 72 hours post-remediation. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-3 (Content Of Audit Records)

Compensating: Validate the authentication fix on FUXA 1.2.11 using curl from a test host: `curl -X POST http://:/api/scheduler -H 'Content-Type: application/json' -d '{"name":"test"}' -v` — a 401 or 403 response confirms enforcement. For OT telemetry monitoring without a commercial solution, configure FUXA's built-in logging at maximum verbosity and pipe output to a syslog server (e.g., rsyslog) for centralized review. Set a cron job to diff the live `schedulers.json` against the known-good backup every 15 minutes and alert on any delta: `diff /opt/fuxa/store/schedulers.json /backup/schedulers_known_good.json && echo 'CLEAN' || echo 'SCHEDULER DRIFT DETECTED'`.

Evidence: Recovery re-enables OT connectivity, which constitutes a significant state change. Before reconnecting OT systems: (1) document the full contents of the restored `schedulers.json` to establish a clean baseline for future diffing; (2) collect a network traffic baseline capture (Wireshark/tcpdump on the FUXA host's OT-facing interface for 15 minutes) immediately after reconnection to establish normal SCADA communication patterns for anomaly comparison during the 72-hour monitoring window; (3) verify FUXA application log timestamps are synchronized (NTP-aligned) so that post-recovery monitoring logs are forensically defensible per NIST AU-8 (Time Stamps).

Step 5: Post-Incident — Conduct a network segmentation review to confirm FUXA and other HMI/SCADA interfaces are not directly internet-reachable. Implement a recurring review of FUXA scheduler configurations as part of OT change management. Evaluate whether authentication controls on all ICS-facing web applications meet the standard required by your OT security policy. Document lessons learned and update the ICS incident response playbook to include FUXA-specific indicators. Reference: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), D3-UAP (User Account Permissions), D3-MFA (Multi-factor Authentication).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without an enterprise NAC or SIEM, conduct the segmentation review manually: use `nmap -Pn -p ` from an external vantage point (e.g., a cloud VM) to confirm FUXA is not internet-reachable post-remediation. For recurring scheduler audits, schedule a weekly cron job that exports the current FUXA scheduler list and emails a diff to the OT administrator. For MFA on FUXA access, deploy Authelia (open source) as an authenticating reverse proxy in front of FUXA if the application itself does not natively support MFA — this adds TOTP enforcement at zero licensing cost.

Evidence: No live-state-altering actions in this phase; however, preserve for lessons-learned documentation: (1) the complete timeline of unauthenticated scheduler API requests extracted from FUXA access logs, annotated with source IPs and scheduler payloads; (2) a before/after comparison of the FUXA scheduler store (pre-exploitation baseline vs. state at detection) to quantify the scope of unauthorized scheduler manipulation; (3) any OT process telemetry anomalies recorded during the exploitation window that can be correlated with unauthorized scheduler execution times, to assess whether physical-process impact occurred.

Detection Guidance

Focus detection efforts on the FUXA application's web access logs and, where available, its internal audit trail. Look for unauthenticated HTTP requests (no valid session cookie or bearer token) to scheduler-related endpoints, typical patterns include POST or PUT requests to paths containing 'scheduler' in the URI, originating from IPs outside the authorized operator network. Any scheduler object created or modified outside of documented change windows warrants immediate investigation. At the network layer, alert on inbound connections to FUXA's listening port from external IP ranges. Cross-reference with MITRE ATT&CK T1190 (exploitation of public-facing application) and ICS T0883 (internet accessible device) detection logic in your SIEM. If your environment uses a SIEM with OT visibility, correlate FUXA scheduler changes against downstream OT process behavior changes. The public proof-of-concept exploit follows a direct unauthenticated API call pattern, so HTTP 200 responses to scheduler endpoints without a preceding authenticated login event are a high-confidence indicator of exploitation. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), D3-SFA (System File Analysis).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/mbanyamer/CVE-2026-25939-SCADA-FUXA-Unauthenticated-Remote-Arbitrary`	Public proof-of-concept exploit repository for CVE-2026-25939; presence of requests matching patterns from this repository in logs indicates active exploitation attempts	HIGH

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter
- **T0883** — Internet Accessible Device

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement

- **AT-2** — Literacy Training and Awareness

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T0883	Internet Accessible Device	Initial-Access

Sources

Source	URL	Tier
vulncheck_kev	https://nvd.nist.gov/vuln/detail/CVE-2026-25939	T1
CVE-2026-25939 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-25939	T3
mbanyamer/CVE-2026-25939-SCADA-FUXA-Unauthenticated ...	https://github.com/mbanyamer/CVE-2026-25939-SCADA-FUXA-Unauthentica...	T3
CVE-2026-25939: Frangoteam FUXA Auth Bypass Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-25939/	T3
Exploit for CVE-2026-25939 - Sploitus	https://sploitus.com/exploit?id=1B4543A7-044D-5DAD-8180-5FD66204347F	T3
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

DISCLAIMER

Generated 2026-06-14 04:23 UTC by TJS Security Command Center