INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 14:06 UTC

CISA ICS Advisory: 12 Vulnerabilities in Anviz Time Clock Products (ICSA-26-106-02)

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0049
Type	CVE Vulnerability
Severity	CRITICAL
Affected Products	Multiple Anviz time clock products (specific models per ICSA-26-106-02)
Published	2026-04-16
Discovery Source	Gemini

Executive Summary

CISA issued ICS advisory ICSA-26-106-02 on April 16, 2026, disclosing 12 vulnerabilities in Anviz time clock devices used for physical access control and workforce management in enterprise and industrial facilities. Specific affected Anviz product lines and firmware versions are documented in the advisory. If exploited individually or in combination, these flaws could allow an attacker to take full control of affected devices, potentially granting unauthorized physical access to secured areas or disrupting workforce operations. Organizations running Anviz time clocks in production environments should treat this as a critical infrastructure risk requiring immediate assessment.

Technical Analysis

CISA advisory ICSA-26-106-02 documents 12 vulnerabilities affecting multiple Anviz time clock product lines. Detailed CVE identifiers, CVSS scores, affected firmware versions, and hardware model numbers are available in the authoritative advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-02 and must be extracted for individual CVE tracking. CVSS scores are pending NVD publication as of the advisory date (2026-04-16); qualitative rating 'critical' is based on vendor severity assessment and exploitation impact (full device control, physical access compromise). MITRE ATT&CK techniques mapped to this advisory include T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), and T1078 (Valid Accounts), suggesting the vulnerability surface spans internet-facing service exploitation, remote access abuse, and credential-based attacks. CWE identifiers are pending extraction from the full advisory. Historical context: a 2019 research post (0x90.zone) documented prior Anviz vulnerabilities under CVE-2019-12393, indicating a recurring pattern of security weaknesses in this product line; those findings are distinct from this advisory. No CISA KEV listing was present as of the advisory date. Patch availability and vendor remediation status were not confirmed in available metadata; consult the CISA advisory and Anviz directly for current patch status.

Action Checklist

1. Step 1: Identify and Isolate, Identify all Anviz time clock devices in your environment using asset inventory or network discovery. Isolate affected devices from internet-facing segments immediately. If devices are accessible remotely, restrict or disable that access until the advisory's specific mitigations are confirmed. Reference ICSA-26-106-02 for affected model numbers and firmware versions.
2. Step 2: Detection, Review network traffic logs for unexpected outbound connections originating from Anviz device IP addresses. Check authentication logs on systems integrated with Anviz time clocks (LDAP, AD, HR platforms) for anomalous login events or account usage outside normal hours. Look for lateral movement from device network segments (T1078, T1133 behavioral indicators).
3. Step 3: Eradication, Retrieve the full advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-02 and contact Anviz directly for firmware patch availability and affected version mapping. Apply vendor-confirmed patches or mitigations per the advisory. If no patch is available, implement network segmentation and disable remote management interfaces as compensating controls.
4. Step 4: Recovery, After patching or applying mitigations, verify device firmware versions match vendor-confirmed safe builds. Re-audit physical access logs for the period since vulnerability disclosure to identify any unauthorized access events. Monitor integrated systems (LDAP, HR platforms) for anomalous account activity for a minimum of 30 days post-remediation.
5. Step 5: Post-Incident Assessment, Evaluate whether Anviz devices are appropriately network-segmented from enterprise IT systems. Assess whether ICS/OT asset inventories are current and include physical access control devices. Review vendor security disclosure processes and ensure future ICS advisories from CISA are routed to the team responsible for physical security infrastructure.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, physical security leadership, and legal/compliance if physical access log review reveals any badge-in events at secured doors that cannot be attributed to authorized personnel during the ICSA-26-106-02 exposure window, or if Anviz device network traffic analysis shows outbound connections to non-Anviz infrastructure suggesting active exploitation — either condition may trigger breach notification obligations under applicable regulations (e.g., HIPAA if healthcare facilities are affected, NERC CIP if electric utility OT environments are in scope).
Recovery Notes	After patching to Anviz-confirmed safe firmware builds, re-validate that all 12 vulnerability classes addressed in ICSA-26-106-02 are remediated by reviewing the advisory's per-CVE mitigation confirmation criteria — do not assume a single firmware update resolves all 12 flaws without vendor confirmation. Monitor the Anviz device VLAN's north-south traffic baseline for 30 days post-patching using NetFlow or firewall logs, flagging any outbound connection attempts to internet-routable addresses since a fully patched device should communicate only with internal authentication backends and NTP servers. Verify that physical access schedules and user account lists on all Anviz devices match authoritative records in your HR and identity systems, as exploitation of these vulnerabilities could have enabled unauthorized modification of access permissions that persists after firmware patching.

Forensic Artifacts	Anviz device internal access event database — badge swipe records (timestamp, card UID, door ID, grant/deny result) exported from the local management server (typically SQLite or MySQL on the Anviz management host); primary record for determining if unauthorized physical access was granted via manipulated door controller logic as a result of ICSA-26-106-02 exploitation. | Network packet captures (PCAP) of traffic to/from Anviz device IPs during the exposure window — specifically any outbound TCP sessions to non-RFC1918 addresses, which would indicate C2 or data exfiltration from a compromised embedded device; capture filter: `host and not net 10.0.0.0/8 and not net 172.16.0.0/12 and not net 192.168.0.0/16`. | Anviz management server web/application logs — HTTP/HTTPS request logs showing admin UI access, firmware upload events, and configuration change events; exploitation of web-based vulnerabilities in the 12-flaw set (e.g., authentication bypass, command injection via web interface) would leave artifact trails in these logs including anomalous URIs, unexpected HTTP methods, or oversized POST bodies. | Windows Security Event Log entries on domain controllers and LDAP servers — specifically Event IDs 4720 (account created), 4722 (account enabled), 4728/4732 (member added to security/local group), and 4776 (NTLM credential validation) filtered for the service accounts used by Anviz LDAP integration; an attacker with control of an Anviz device could leverage the integration credential to make directory queries or, if the service account is over-privileged, to create or elevate accounts. | Anviz device firmware image hash — SHA-256 hash of the currently installed firmware binary (extracted pre-patch via TFTP or vendor maintenance mode if supported) compared against Anviz's published hash for the affected and safe-build versions; confirms whether the device is running unmodified vendor firmware or a tampered image that could persist post-patch.

Per-Action IR Details

Step 1: Containment — Identify all Anviz time clock devices in your environment using asset inventory or network discovery. Isolate affected devices from internet-facing segments immediately. If devices are accessible remotely, restrict or disable that access until the advisory's specific mitigations are confirmed. Reference ICSA-26-106-02 for affected model numbers and firmware versions.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment, Eradication, and Recovery: Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run a targeted nmap scan against your OT/physical access VLAN to enumerate Anviz devices by open ports typical to these time clocks (TCP 80, 443, 8080, and vendor-specific management ports): `nmap -sV -p 80,443,8080,4370 --open 192.168.X.0/24 -oN anviz_discovery.txt`. Cross-reference discovered IPs against your DHCP lease logs. Use iptables or firewall ACLs to immediately block all inbound and outbound internet-routable traffic to/from discovered Anviz device IPs: `iptables -I FORWARD -s -j DROP && iptables -I FORWARD -d -j DROP`. Disable any port-forwarding rules for Anviz management interfaces on perimeter firewalls.

Evidence: Before isolating, capture full packet headers for any active sessions to/from Anviz device IPs using `tcpdump -i host -w anviz_preflight_$(date +%F).pcap`. Pull ARP tables (`arp -a`) and switch CAM table entries to confirm physical port assignments. Export current firewall rule sets and NAT tables to document whether remote management interfaces (e.g., web UI, SSH, proprietary Anviz management protocol ports) were internet-accessible prior to containment — this establishes pre-exploitation exposure window for ICSA-26-106-02.

Step 2: Detection — Review network traffic logs for unexpected outbound connections originating from Anviz device IP addresses. Check authentication logs on systems integrated with Anviz time clocks (LDAP, AD, HR platforms) for anomalous login events or account usage outside normal hours. Look for lateral movement from device network segments (T1078, T1133 behavioral indicators).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Signs of an Incident

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: For network traffic analysis without a SIEM, use Wireshark or tcpdump to capture traffic from the Anviz device VLAN and filter for outbound connections to non-expected destinations: `tcpdump -r anviz_capture.pcap 'src net and not dst net '`. For AD/LDAP anomaly detection, query Windows Security Event Log for Event ID 4624 (successful logon) and 4625 (failed logon) filtering on source IPs matching Anviz device addresses: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625) -and $_.Message -match ''}`. For T1133 (External Remote Services) indicators, review VPN and remote access gateway logs for authentication attempts originating from Anviz device IPs or accounts associated with time clock integration service accounts. Use Zeek (formerly Bro) on a network tap to baseline Anviz device communication patterns and flag deviations.

Evidence: Capture and preserve: (1) NetFlow or firewall connection logs for the 30-day window prior to ICSA-26-106-02 disclosure (April 16, 2026) showing all outbound sessions from Anviz device IPs — exfiltration or C2 callbacks from an embedded device would appear as low-volume, periodic outbound connections to non-Anviz cloud infrastructure. (2) Windows Security Event Log entries (Event IDs 4768, 4769 — Kerberos ticket requests; 4776 — NTLM authentication) on domain controllers, filtered for the service accounts used by Anviz LDAP/AD integration, looking for off-hours or geographically impossible authentications. (3) HR platform access logs (e.g., ADP, Kronos/UKG, SAP HCM) for API calls or login events tied to the Anviz integration service account, which an attacker with device control could leverage to manipulate workforce records.

Step 3: Eradication — Retrieve the full advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-02 and contact Anviz directly for firmware patch availability and affected version mapping. Apply vendor-confirmed patches or mitigations per the advisory. If no patch is available, implement network segmentation and disable remote management interfaces as compensating controls.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery: Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If Anviz has not yet released patches for all 12 vulnerabilities in ICSA-26-106-02, implement the following without a patch management platform: (1) Disable the Anviz web management interface by blocking TCP 80/443 to device IPs at the access-layer switch using port ACLs. (2) If the devices expose a remote management protocol (SSH, Telnet, proprietary), disable it via the device's local console interface and document the change. (3) Place Anviz devices on an isolated VLAN with a default-deny firewall policy allowing only the minimum required communication: device-to-time-server (NTP UDP 123), device-to-authentication-backend (only required port/IP), and admin workstation-to-device for local management. Document VLAN assignment and ACL rules as your compensating control record for audit purposes.

Evidence: Before applying firmware patches, image the current device filesystem if the Anviz hardware supports it (check vendor documentation for maintenance mode or TFTP firmware extraction). At minimum, record the current firmware version string from the device admin UI or via SNMP OID query (`snmpwalk -v2c -c public 1.3.6.1.2.1.1.1`) and preserve it. Export the device's current configuration, user account list, and access schedule data — if an attacker exploited ICSA-26-106-02 to implant a backdoor account or modify access schedules, this pre-patch snapshot is the forensic baseline. Compute SHA-256 hashes of any firmware files before and after patching to verify integrity of the vendor-supplied patch.

Step 4: Recovery — After patching or applying mitigations, verify device firmware versions match vendor-confirmed safe builds. Re-audit physical access logs for the period since vulnerability disclosure to identify any unauthorized access events. Monitor integrated systems (LDAP, HR platforms) for anomalous account activity for a minimum of 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Post-Incident Activity: Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Verify firmware integrity post-patch by querying the device management interface for the firmware version string and comparing against the Anviz-confirmed safe build listed in ICSA-26-106-02 or vendor patch notes — document with a screenshot or CLI output. For physical access log re-audit without a PACS SIEM: export raw access event logs from the Anviz management server database (typically a local SQLite or MySQL instance) and run a query for all badge-in events during the exposure window sorted by user, time, and door — flag any entries for accounts not recognized in your HR system, access to high-security doors outside business hours, or sequential badge use that is physically impossible (tailgating indicator). Use osquery on systems integrated with Anviz (LDAP servers, HR application servers) to establish a 30-day monitoring baseline: `SELECT * FROM last WHERE time > (strftime('%s','now') - 2592000);` to track unusual login sessions.

Evidence: Pull and preserve the Anviz device's internal access event log (badge swipe records with timestamp, card UID, door ID, and grant/deny status) for the full period from 90 days before ICSA-26-106-02 disclosure through the patch date — this is the primary forensic record for determining whether unauthorized physical access occurred as a result of exploitation. Separately collect physical security camera footage indexes (not necessarily full video) for controlled entry points served by affected Anviz readers for the same window. Retain LDAP/AD audit logs (Windows Event IDs 4720, 4728, 4732 — account creation and group membership changes) for the integration service accounts, as exploitation of these devices could enable privilege escalation into directory services.

Step 5: Post-Incident — Evaluate whether Anviz devices are appropriately network-segmented from enterprise IT systems. Assess whether ICS/OT asset inventories are current and include physical access control devices. Review vendor security disclosure processes and ensure future ICS advisories from CISA are routed to the team responsible for physical security infrastructure.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST IR-3 (Incident Response Testing), NIST IR-6 (Incident Reporting), NIST RA-3 (Risk Assessment), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Formalize ICS/physical access control device inclusion in your asset inventory using a free CMDB approach: add Anviz device records to a shared spreadsheet or wiki with fields for model, firmware version, network location, VLAN assignment, physical door/location served, and responsible owner (physical security vs. IT). Create a CISA ICS-CERT RSS feed subscription (`https://www.cisa.gov/ics-advisories.xml`) routed to the physical security team's email distribution list so future advisories for physical access control vendors are not filtered to IT-only queues. Draft a one-page network segmentation standard for physical access control devices specifying that PACS hardware must reside on a dedicated VLAN with no direct routing to enterprise IT subnets, enforced by ACL.

Evidence: Document the lessons-learned record for this incident per NIST 800-61r3 §4, including: the date ICSA-26-106-02 was published versus the date your team received and acted on it (measures advisory-to-action latency), the number of Anviz devices discovered versus the number previously inventoried (measures asset visibility gap), and whether any physical access events during the exposure window remain unexplained after log review. This record supports future risk assessments under NIST RA-3 (Risk Assessment) and provides audit evidence that the organization responded to a CISA critical ICS advisory. Retain all forensic artifacts collected during Steps 1–4 per your record retention policy, with a minimum recommendation of one year given the physical security implications of ICSA-26-106-02.

Detection Guidance

Specific IOC signatures, individual CVE identifiers, and exploit patterns are pending extraction from the full ICSA-26-106-02 advisory. Detection should focus on behavioral indicators aligned with the mapped ATT&CK techniques. For T1190 (Exploit Public-Facing Application): monitor web application and device management interface logs for unexpected request patterns, error spikes, or authentication bypass attempts targeting Anviz device management ports. For T1133 (External Remote Services): alert on inbound connections to Anviz device management interfaces from external IP ranges; Anviz time clocks should not accept management traffic from the internet. For T1078 (Valid Accounts): correlate Anviz device authentication events with HR and AD logs to detect accounts logging into physical access systems outside normal business hours or from unexpected source IPs. Query your SIEM for Anviz device hostnames or IP addresses as traffic sources to internal systems they should not reach. The full advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-106-02 should be consulted for any vendor-specific detection signatures or IOCs.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1133** — External Remote Services
- **T1078** — Valid Accounts

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
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1133	External Remote Services	Persistence

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
gemini	https://waterisac.org/articles/tlpclear-cisa-ics-advisories-additio...	T3
Anviz Devices Under Threat Researchers discovered critical ...	https://www.instagram.com/p/DXNJDkvl-hB/	T3
Anviz Pwn! How broken devices could be? (CVE-2019-12393 ... - 0x90	https://www.0x90.zone/multiple/reverse/2019/11/28/Anviz-pwn.html	T3
Lifetime Support Cloud-based Time and Attendance Solution - Anviz	https://www.anviz.com/cloud-based-time-and-attendance-solution-cros...	T3
Notice about Vulnerability in EZVIZ NAS products	https://www.ezviz.com/newsroom/notice+about+vulnerability+in+ezviz+...	T3

Generated 2026-04-17 14:06 UTC by TJS Security Command Center