INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-01 15:53 UTC

CISA Advisory: Three Vulnerabilities in Daktronics Controller Firmware Enable Remote Manipulation of Highway Signs and Billboards

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0313
Type	Security Analysis
Severity	HIGH
Affected Products	Daktronics Controller Firmware (specific versions not confirmed from available sources)
Published	2026-06-30
Discovery Source	Gemini

Executive Summary

CISA has issued ICS advisory ICSA-26-176-04 identifying three vulnerabilities in Daktronics controller firmware used in highway signs, billboards, and related public-facing infrastructure. According to the advisory, the flaws could allow remote attackers to manipulate displayed messaging on those signs, potentially enabling traffic disruption or public deception campaigns. Organizations operating Daktronics-controlled signage infrastructure should prioritize firmware updates per the CISA advisory and review network access controls for affected OT assets.

Technical Analysis

CISA advisory ICSA-26-176-04 identifies three vulnerabilities in Daktronics controller firmware deployed in highway signs, billboards, and related operational technology. Specific CVE identifiers and CVSS scores are available in the CISA advisory and GitHub advisory (see sources). MITRE ATT&CK techniques mapped to this advisory include T1491.002 (Defacement: External Defacement), T1498 (Network Denial of Service), and T1565 (Data Manipulation). The attack vector is described as remote. No CWE identifiers were confirmed from available sources. Remediation path per the advisory is firmware update; specific patch version and update procedure should be obtained directly from the CISA advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-04 and validated against the Daktronics vendor advisory.

Action Checklist

1. Step 1: Containment, Identify all Daktronics controller firmware deployments in your OT environment (highway signs, billboards, and related public-facing signage assets). Isolate affected controllers from internet-facing network segments where operationally feasible, pending firmware update. Reference CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory to confirm all Daktronics assets are inventoried.
2. Step 2: Detection, Review network logs for unexpected inbound connections to Daktronics controller management interfaces. Check SIEM for anomalous commands or configuration changes pushed to signage controllers. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) to query logs for access events on controller management ports. Apply NIST AC-2 (Account Management) to detect unauthorized account activity on controller interfaces. Note: specific event IDs and log query strings depend on the controller model and management platform; consult Daktronics documentation for controller-specific logging guidance.
3. Step 3: Eradication, Apply the firmware update identified in CISA advisory ICSA-26-176-04. Obtain the specific firmware version and update procedure directly from CISA (https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-04) and the Daktronics vendor advisory. Apply CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) processes to track and verify update completion across all affected controllers.
4. Step 4: Recovery, After firmware update, verify controller messaging output against expected baseline content. Monitor signage controllers for unauthorized content changes post-remediation using NIST SI-4 equivalent OT monitoring where available. Apply NIST AU-3 (Content Of Audit Records) to confirm post-update audit logging is intact and capturing controller access events. Validate network segmentation controls remain in place.
5. Step 5: Post-Incident, Review OT network segmentation posture for all public-facing signage infrastructure. Assess whether Daktronics controllers are reachable from external networks and implement network-layer access controls to restrict management interface exposure. Apply NIST AC-2 (Account Management) to enforce least-privilege access on controller accounts. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) for network-level controls. Update the asset inventory (CIS 1.1) and vulnerability management process (CIS 7.1) to include OT/ICS firmware assets going forward.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to OT security leadership and (where applicable) state DOT or infrastructure owner if network logs confirm any inbound connection to Daktronics controller management interfaces from non-organizational IPs, or if any controller displays unauthorized message content — both conditions indicate potential active exploitation of ICSA-26-176-04 on public-safety infrastructure and may trigger CISA ICS incident reporting obligations under CIRCIA.

Recovery Notes	After firmware update, verify each Daktronics controller is displaying only approved, scheduled message content by cross-referencing live sign output against the Venus Control Suite message schedule — any deviation indicates either residual attacker configuration or incomplete update. Monitor OT management VLAN traffic for at least 30 days post-remediation for reconnection attempts to controller management ports from previously observed suspicious source IPs. Given the public-safety nature of highway signage infrastructure, maintain enhanced monitoring through at least one full traffic-cycle season (typically 90 days) to confirm no latent persistence mechanism survived the firmware update.
Forensic Artifacts	Daktronics Venus Control Suite (or equivalent management platform) event logs: configuration change history, login/logout events, and message schedule push events — these will show if an attacker remotely modified displayed content or controller parameters during the exploitation window. | OT network management VLAN packet capture (pcap): inbound TCP session records to Daktronics controller management ports, preserving source IP, timestamp, session duration, and payload size — the primary network-layer evidence of remote exploitation attempts against ICSA-26-176-04 affected firmware. | Controller firmware version strings and configuration backups pre-update: exported from each affected controller before patching, documenting both the vulnerable firmware state and any attacker-injected message schedules or network parameter modifications that may have been introduced through the vulnerability. | Firewall and router ACL logs for the OT network boundary: records of inbound connection attempts to controller management port ranges from internet-sourced IPs, covering the 90-day window prior to CISA advisory publication to establish whether exploitation preceded the advisory. | Physical or remote-capture screenshots of sign display content at time of incident discovery: documents any unauthorized messaging (traffic disruption text, public deception content) as evidence of successful remote manipulation, which may be relevant for regulatory reporting or law enforcement referral under CIRCIA or state DOT incident notification requirements.

Per-Action IR Details

Step 1: Containment — Identify all Daktronics controller firmware deployments in your OT environment (highway signs, billboards, and related public-facing signage assets). Isolate affected controllers from internet-facing network segments where operationally feasible, pending firmware update. Reference CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory to confirm all Daktronics assets are inventoried.

NIST Phase: Containment

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), NIST IR-4 (Incident Handling)

Compensating: Use nmap or Shodan CLI (shodan search 'Daktronics') to enumerate any Daktronics management interfaces exposed to internet-facing segments. On the OT network, run 'arp -a' or a passive Wireshark capture on the management VLAN to enumerate active controller IPs without generating disruptive traffic. Document each controller by IP, MAC, physical location, and sign ID in a spreadsheet before any isolation action.

Evidence: Before isolating any controller, capture: (1) active TCP connection state on the management interface via 'netstat -ano' or Wireshark packet capture on the OT management VLAN — preserve any established inbound sessions that could indicate active attacker presence; (2) controller management interface access logs (Daktronics Venus Control Suite or equivalent) showing recent login events and configuration push history; (3) ARP table snapshot of the OT network segment to identify any unexpected hosts communicating with controller IPs.

Step 2: Detection — Review network logs for unexpected inbound connections to Daktronics controller management interfaces. Check SIEM for anomalous commands or configuration changes pushed to signage controllers. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) — query logs for access events

on controller management ports. Apply D3-LAM (Local Account Monitoring) to detect unauthorized account activity on controller interfaces. Note: specific event IDs and log query strings depend on the controller model and management platform; consult Daktronics documentation for controller-specific logging guidance.

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-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, deploy Wireshark or tcpdump on a span/mirror port of the OT management VLAN and capture 24–48 hours of traffic; filter for inbound connections to known Daktronics controller IPs on management ports (typically TCP 7000, 7001, or vendor-specific ports — confirm in Daktronics Venus Control Suite documentation). Use 'grep' against exported Venus Control Suite or NTCIP-based management logs to identify configuration-change events outside scheduled maintenance windows. For internet-exposed controllers, query firewall or router logs for inbound connections originating from non-organizational IPs to controller management ports.

Evidence: Capture before any account lockout or session revocation: (1) active sessions on Daktronics controller management interfaces — export current session list from Venus Control Suite or equivalent management platform; (2) network flow records (NetFlow/sFlow) or firewall logs showing source IPs, timestamps, and byte counts for inbound connections to controller management ports in the 30 days prior to advisory publication (ICSA-26-176-04 issued 2026); (3) controller configuration change audit trail — Daktronics management software logs showing message schedule modifications, firmware parameter changes, or administrative login events; (4) DNS query logs from OT network resolvers for any unusual external domains resolved by controller IPs.

Step 3: Eradication — Apply the firmware update identified in CISA advisory ICSA-26-176-04. Obtain the specific firmware version and update procedure directly from CISA (https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-04) and the Daktronics vendor advisory, as specific patch identifiers were not confirmed in available sources. Apply CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) processes to track and verify update completion across all affected controllers.

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), NIST IR-4 (Incident Handling)

Compensating: Without automated patch management tooling for OT firmware, maintain a manual tracking spreadsheet: controller asset ID, current firmware version (read from Daktronics Venus Control Suite or direct controller interface), target firmware version per CISA advisory, update date, and technician sign-off. Stage firmware update files on an isolated laptop — do not transfer via internet-connected media. Verify firmware integrity using the hash values published in the Daktronics vendor advisory before applying. For controllers that cannot be updated immediately due to operational constraints (24/7 highway signage), document the exception with a compensating isolation control and a target remediation date.

Evidence: Before applying the firmware update (which overwrites controller flash storage and destroys current firmware state): (1) capture the current firmware version string from each controller via the Daktronics management interface — document as baseline evidence of the vulnerable state; (2) export the full controller configuration backup (message schedules, display parameters, network settings) from Venus Control Suite — this documents the pre-update state and detects any attacker-injected configuration; (3) capture a final network packet capture on the controller management port to preserve any residual attacker session artifacts before the update process terminates active connections; (4) preserve controller system logs (syslog output if configured, or management platform event logs) to a write-once or offsite location before the update process may overwrite them.

Step 4: Recovery — After firmware update, verify controller messaging output against expected baseline content. Monitor signage controllers for unauthorized content changes post-remediation using NIST SI-4

equivalent OT monitoring where available. Apply NIST AU-3 (Content Of Audit Records) to confirm post-update audit logging is intact and capturing controller access events. Validate network segmentation controls remain in place.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-3 (Content Of Audit Records), NIST AU-2 (Event Logging), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Physically inspect or remotely screenshot each updated Daktronics sign's current displayed content against the approved message schedule — flag any deviation as a potential indicator of persistent compromise or residual configuration tampering. Re-run the tcpdump/Wireshark capture on the OT management VLAN post-update to confirm no inbound connections are reaching controller management ports from unexpected source IPs. Verify firewall or ACL rules blocking internet-originated traffic to controller management ports are still enforced by attempting a connection from an external test IP and confirming refusal.

Evidence: Post-update verification artifacts to preserve as recovery evidence: (1) firmware version confirmation screenshot or log export from each updated controller, documenting the new firmware version string as proof of successful patching; (2) post-update configuration export from Venus Control Suite to confirm attacker-injected message schedules or display parameters were not preserved through the firmware update process; (3) network segmentation validation log — firewall rule audit or ACL review confirming controller management ports are not reachable from internet-facing segments post-remediation; (4) post-update audit log sample from each controller confirming logging is active and recording access events (per NIST AU-3), as firmware updates on embedded OT devices sometimes reset logging configurations to factory defaults.

Step 5: Post-Incident — Review OT network segmentation posture for all public-facing signage infrastructure. Assess whether Daktronics controllers are reachable from external networks and implement network-layer access controls to restrict management interface exposure. Apply D3-UAP (User Account Permissions) to enforce least-privilege access on controller accounts. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) for network-level controls. Update the asset inventory (CIS 1.1) and vulnerability management process (CIS 7.1) to include OT/ICS firmware assets going forward.

NIST Phase: Post Incident

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), NIST IR-8 (Incident Response Plan)

Compensating: Use Shodan CLI or Censys free tier to re-query for any Daktronics management interfaces still internet-exposed post-remediation ('shodan search port:7000 Daktronics' or equivalent). Conduct a lessons-learned meeting within 2 weeks of containment; document findings in a one-page after-action report covering detection gap (why were these controllers not in the firmware asset inventory?), dwell time estimate (earliest evidence of potential exploitation vs. advisory date), and segmentation gaps. Update the OT asset inventory to include firmware version as a tracked field, and add Daktronics CISA ICS advisories to the team's recurring threat intelligence feed monitoring (CISA ICS-CERT RSS or email subscription).

Evidence: Post-incident documentation artifacts: (1) completed asset inventory update confirming all Daktronics controllers are enumerated with firmware version, network segment, and physical location — this becomes the baseline for future ICS advisory triage; (2) network segmentation validation report confirming management interfaces are firewalled from internet-facing segments and restricted to authorized management workstation IPs only; (3) account audit export from Daktronics management platform confirming all controller accounts follow least-privilege assignment and any default or shared credentials have been rotated post-incident; (4) after-action report documenting timeline from advisory publication to full remediation, including any operational windows where controllers remained vulnerable due to 24/7 sign uptime constraints.

Detection Guidance

Monitor network traffic to and from Daktronics controller management interfaces for unexpected inbound connections, particularly from external IP ranges. Review controller access logs for unauthorized login attempts or configuration changes, apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) frequency requirements to these log sources. Apply NIST SI-7 (Software, Firmware, and Information Integrity) to detect unauthorized modification of controller configuration files or firmware. Apply NIST AC-2 (Account Management) to identify anomalous account activity on controller management planes. Specific log query strings and event IDs will vary by Daktronics controller model and management software version; consult Daktronics documentation for platform-specific guidance. No confirmed IOCs (IP addresses, domains, hashes) were available from sources verified during this analysis.

Framework Mappings

MITRE-ATTACK

- **T1491.002** — External Defacement
- **T1498** — Network Denial of Service
- **T1565** — Data Manipulation

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1491.002	External Defacement	Impact
T1498	Network Denial of Service	Impact
T1565	Data Manipulation	Impact

Sources

Source	URL	Tier
Daktronics Controller Firmware - CISA	https://www.cisa.gov/news-events/ics-advisories/icsa-26-176-04	T1
New Controller Flaws Expose Highway Signs and Billboards to ...	https://www.securityweek.com/new-controller-flaws-expose-highway-si...	T2

Source	URL	Tier
Daktronics Updates Controller Firmware - ISSSource	https://www.isssource.com/daktronics-updates-controller-firmware/	T3
Daktronics Controller Firmware - vulnerability database	https://vulners.com/ics/ICSA-26-176-04	T3
Various versions of Daktronics Controller Firmware could... - GitHub	https://github.com/advisories/GHSA-qr6g-wmfj-4xhv	T1

Generated 2026-07-01 15:53 UTC by TJS Security Command Center