INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-30 14:09 UTC

ABB OPTIMAX Authentication Bypass Exposes Critical Infrastructure to Unauthenticated Access via Azure AD SSO Flaw

CVE VULNERABILITY | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0103
Type	CVE Vulnerability
CVE ID	CVE-2025-14510
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0003 (9th percentile)
Affected Products	ABB Ability OPTIMAX 6.1 (all versions, no fix available), 6.2 (all versions, no fix available), 6.3 (< 6.3.1-251120), 6.4 (< 6.4.1-251120)
Published	2026-04-30T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

A critical authentication bypass vulnerability (CVE-2025-14510) in ABB Ability OPTIMAX allows unauthenticated remote attackers to gain access to energy management systems without valid credentials. The flaw affects OPTIMAX versions 6.1 through 6.4, with no patch available for versions 6.1 and 6.2. Organizations in energy and water/wastewater sectors running affected versions face confirmed exposure to unauthenticated remote access to operational technology systems controlling critical infrastructure.

Technical Analysis

CVE-2025-14510 is an authentication bypass in ABB Ability OPTIMAX energy management and optimization software, classified under CWE-303 (Incorrect Implementation of Authentication Algorithm). The flaw exists in deployments configured to use Azure Active Directory Single Sign-On (SSO). An unauthenticated remote attacker can bypass authentication controls entirely, gaining access without valid credentials. CVSS v3.1 base score is 8.1 per the CVE record; NVD publication is pending. EPSS score is 0.031% (percentile rank 0.088), indicating very low current exploitation probability across the active vulnerability landscape, though the OT/critical infrastructure context elevates operational risk independent of EPSS. Affected versions: 6.1 (all builds, no patch available), 6.2 (all builds, no patch available), 6.3 (builds earlier than 6.3.1-251120, patch available), 6.4 (builds earlier than 6.4.1-251120, patch available). MITRE ATT&CK techniques: T1078 (Valid

Accounts), T1190 (Exploit Public-Facing Application), T1556 (Modify Authentication Process), T1133 (External Remote Services), T1199 (Trusted Relationship). Primary advisory: CISA ICS Advisory ICSA-26-120-04. NVD record: CVE-2025-14510.

Action Checklist

1. Containment: Immediately inventory all OPTIMAX deployments and identify versions. For versions 6.1 and 6.2 (no patch available), isolate systems from external network access and enforce network-layer access controls (firewall rules, jump host requirements) to block unauthenticated remote reach. Disable Azure AD SSO configuration on affected instances where operationally feasible. Reference CISA ICS Advisory ICSA-26-120-04 for detailed vendor guidance.
2. Detection: Audit Azure AD sign-in logs and OPTIMAX application logs for authentication events lacking valid SSO token issuance or showing successful access with anomalous or absent credential validation. Look for access from unexpected IP ranges or at unusual hours. Review ICS historian and SCADA integration logs for unauthorized read/write activity post-access. No public IOC signatures or exploit code are available at this time; focus on behavioral and log-based detection (see Detection Guidance section).
3. Eradication: For OPTIMAX 6.3, upgrade to build 6.3.1-251120 or later. For OPTIMAX 6.4, upgrade to build 6.4.1-251120 or later. For versions 6.1 and 6.2, no vendor patch exists; contact ABB Technical Support or your account team, reference CISA ICS Advisory ICSA-26-120-04 and CVE-2025-14510, and request a migration timeline to a supported build. After patching, revoke and reissue all active Azure AD SSO sessions for OPTIMAX and force reauthentication.
4. Recovery: After patching or isolation, verify authentication flows by testing SSO login with valid and invalid credentials to confirm the bypass no longer succeeds. Review OPTIMAX audit logs for any unauthorized configuration changes or data access that may have occurred during the exposure window. Restore normal network access only after confirming the patched build is active and authentication is functioning correctly.
5. Post-Incident: This vulnerability exposes a gap in OT authentication architecture: SSO integrations in ICS environments require the same security validation rigor as core authentication systems. Assess all other OT/ICS platforms using federated identity or SSO for similar misconfigurations. Review network segmentation controls to confirm ICS-facing applications are not directly internet-accessible. Update asset inventory to track OPTIMAX version and patch status on a recurring basis.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, OT security leadership, and legal/compliance immediately if Azure AD sign-in logs or OPTIMAX application logs show any successful session established without a correlated valid SSO token during the exposure window, or if OPTIMAX is deployed in a NERC CIP or AWIA 2018-regulated environment where unauthorized access to energy management or water control systems triggers mandatory incident reporting obligations.

Recovery Notes	After applying patches to OPTIMAX 6.3 and 6.4, monitor Azure AD Sign-in Logs and OPTIMAX application logs continuously for a minimum of 30 days for anomalous authentication patterns, including any re-attempt of the bypass vector (direct session creation without Azure AD redirect). For OPTIMAX 6.1 and 6.2 instances remaining in isolated operation pending ABB migration, implement weekly manual review of all network connection logs to the isolated segment and verify firewall rules remain intact. Do not restore external network access to any OPTIMAX instance until the patched build is confirmed active via binary hash comparison and authentication validation testing is documented.
Forensic Artifacts	Azure AD (Entra ID) Sign-in Logs for the OPTIMAX enterprise application registration — specifically rows where 'Authentication Requirement' shows success but no corresponding SAML assertion ID or OAuth token ID is logged, indicating the bypass condition was triggered; export raw JSON before 7-day (free) or 30-day (P1/P2) retention expires. | OPTIMAX application-level session and access logs (located in the ABB OPTIMAX install directory per vendor documentation) — preserve the full log set covering from last known-clean date through isolation, filtering for session_created or login_success events with no associated Azure AD token reference. | ICS historian audit trail (OSIsoft PI, Honeywell Uniformance, or equivalent integrated with OPTIMAX) — extract all write transactions to energy management data points (setpoints, dispatch schedules, load commands) initiated from the OPTIMAX process context during the exposure window, cross-referenced against authorized operator work orders. | Perimeter and host-based firewall logs for the OPTIMAX server's listener port (HTTP/HTTPS) — network flow data showing external IP sources that established successful TCP sessions to the OPTIMAX web interface, particularly those not originating from the corporate jump host or VPN egress ranges, as the authentication bypass would produce a completed TCP handshake and HTTP 200 response without Azure AD redirect. | Windows Security Event Log (Event ID 4624 — Successful Logon, Logon Types 3 and 10) and Event ID 4648 (Explicit Credential Logon) on the OPTIMAX host — these would capture any OS-level account activity initiated by an attacker who gained OPTIMAX application access and attempted lateral movement or privilege escalation within the ICS network segment.

Per-Action IR Details

Containment — Immediately inventory all OPTIMAX deployments and identify versions. For versions 6.1 and 6.2 (no patch available), isolate systems from external network access and enforce network-layer access controls (firewall rules, jump host requirements) to block unauthenticated remote reach. Disable Azure AD SSO configuration on affected instances where operationally feasible. Reference CISA ICS Advisory ICSA-26-120-04 for vendor guidance.

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), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 (Establish and Maintain a Secure Network Architecture) — enforce network segmentation isolating OPTIMAX from internet-facing segments, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For teams without a network management platform: use 'netstat -an' or 'ss -tulnp' on the OPTIMAX host to enumerate active listening ports and established connections, then apply host-based Windows Firewall rules via PowerShell ('New-NetFirewallRule -DisplayName Block-OPTIMAX-External -Direction Inbound -RemoteAddress -Action Block') to restrict inbound access to jump-host IPs only. Disable the Azure AD SSO configuration by modifying the OPTIMAX application configuration file (consult ABB documentation for the SSO config path) and restarting the OPTIMAX service. Document every firewall rule change with timestamp and approver for the incident record.

Evidence: Before isolating, capture a full netstat snapshot ('netstat -anob > netstat_pre_isolation.txt') showing all active TCP connections to OPTIMAX listener ports — this preserves any attacker sessions active at time of discovery.

Export the OPTIMAX application server's current Azure AD SSO configuration file (location per ABB install path) to document the misconfigured state. Pull the host's ARP cache ('arp -a') and DNS cache ('ipconfig /displaydns') to identify any attacker-controlled infrastructure that communicated with the OPTIMAX host prior to isolation.

Detection — Audit Azure AD sign-in logs and OPTIMAX application logs for authentication events lacking valid SSO token issuance or showing successful access with anomalous or absent credential validation. Look for access from unexpected IP ranges or at unusual hours. Review ICS historian and SCADA integration logs for unauthorized read/write activity post-access. No public IOC signatures are available at this time.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: In Azure AD (Entra ID), navigate to Sign-in Logs and filter by Application = 'ABB OPTIMAX' (or the registered app display name in your tenant); export to CSV and grep for rows where 'Authentication Requirement' is satisfied but 'MFA Result' is blank or 'Token Protection' is absent — these indicate the bypass condition. On the OPTIMAX application server, locate the application log directory (default path per ABB documentation) and search for session creation events with no corresponding SAML assertion or OAuth token receipt: 'Select-String -Path .*.log -Pattern "session_created|login_success" | Where-Object { $_ -notmatch "token_id|assertion_id" }'. For ICS historian (e.g., OSIsoft PI or Honeywell Uniformance), query for write transactions in the exposure window from the OPTIMAX service account or any non-standard initiator.

Evidence: Capture and preserve: (1) Azure AD Sign-in Logs for the OPTIMAX application registration scoped to the full exposure window — export raw JSON from the Entra ID portal before log retention expires (default 30 days for P1/P2, 7 days free tier). (2) OPTIMAX application-level access logs showing session tokens issued, source IPs, and authenticated usernames — flag any session where no valid Azure AD token correlation exists. (3) ICS historian audit trail for read/write operations against energy management data points (setpoints, load schedules, dispatch commands) initiated during the exposure window from OPTIMAX process context. (4) Network flow data (NetFlow/IPFIX from perimeter firewall) for OPTIMAX listener port traffic from external IP ranges — the authentication bypass means a successful TCP session to the OPTIMAX web interface without a redirect to Azure AD login constitutes a high-confidence exploit indicator.

Eradication — For OPTIMAX 6.3, upgrade to build 6.3.1-251120 or later. For OPTIMAX 6.4, upgrade to build 6.4.1-251120 or later. For versions 6.1 and 6.2, no vendor patch exists — coordinate with ABB directly regarding migration path to a supported version. After patching, revoke and reissue all active Azure AD SSO sessions for OPTIMAX and force reauthentication.

NIST Phase: Eradication

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

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST CM-3 (Configuration Change Control), NIST IA-5 (Authenticator Management), 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: Before applying the ABB patch to OPTIMAX 6.3 or 6.4, take a full VM snapshot or disk image of the OPTIMAX host as a pre-patch forensic baseline. Apply the upgrade to build 6.3.1-251120 or 6.4.1-251120 per ABB's upgrade procedure (obtain from ABB support portal or ICSA-26-120-04 guidance). Post-upgrade, revoke all active OPTIMAX SSO sessions via Azure AD: in Entra ID admin center, navigate to Enterprise Applications > [OPTIMAX app] > Users and Groups, then use 'Revoke Sessions' for all assigned users, or run: 'Get-MgUser -All | ForEach-Object { Revoke-MgUserSignInSession -UserId $_.Id }' (requires Microsoft.Graph PowerShell module). For 6.1/6.2 with no patch, document ABB's written response regarding migration timeline and treat these instances as permanently compromised pending migration.

Evidence: Before patching, collect: (1) OPTIMAX application binary hash (SHA-256) of the current executable and core DLLs to establish the vulnerable-version baseline for post-patch comparison ('Get-FileHash -Algorithm SHA256 -Path *.exe,*.dll | Export-Csv pre_patch_hashes.csv'). (2) A dump of all currently active Azure AD SSO sessions for the OPTIMAX application registration via Entra ID Sign-in Logs — this captures any attacker-maintained session

tokens that must be invalidated. (3) Windows Event Log — Security (Event ID 4624, Logon Type 3/10) from the OPTIMAX host covering the exposure window to identify any accounts used to authenticate to the system during the bypass period.

Recovery — After patching or isolation, verify authentication flows by testing SSO login with valid and invalid credentials to confirm bypass no longer succeeds. Review OPTIMAX audit logs for any unauthorized configuration changes or data access that may have occurred during the exposure window. Restore normal network access only after confirming patched build is active and authentication is functioning correctly.

NIST Phase: Recovery

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

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Perform authentication validation testing using two test accounts: one with valid Azure AD credentials provisioned for OPTIMAX, and one with no OPTIMAX entitlement. Attempt login with both and confirm the unentitled account receives a proper denial with a corresponding Azure AD sign-in log entry showing failure reason 'AADSTS50105' (user not assigned to application) rather than a successful session. Use curl or a browser developer console to confirm that the OPTIMAX login flow triggers a proper Azure AD SAML/OIDC redirect rather than allowing direct session creation: 'curl -v -L https://:/login 2>&1 | grep -E "Location|Set-Cookie|200 OK"' — a 302 redirect to login.microsoftonline.com confirms SSO enforcement is active. Compare current OPTIMAX application binary hashes against the pre-patch baseline captured during eradication.

Evidence: Before restoring network access, collect: (1) OPTIMAX audit log export covering the full exposure window (from initial public disclosure or last known-clean date through isolation) — review specifically for configuration changes to energy dispatch setpoints, load profiles, or SCADA integration endpoints that an unauthenticated attacker could have modified. (2) ICS historian trend data for all process variables writable via OPTIMAX during the exposure window — abnormal step-changes in setpoints without corresponding operator work orders are indicators of unauthorized manipulation. (3) Post-patch authentication test results (pass/fail for valid and invalid credential scenarios) documented with timestamps and tester identity for the incident record.

Post-Incident — This vulnerability exposes a gap in OT authentication architecture: SSO integrations in ICS environments require the same security validation rigor as core authentication systems. Assess all other OT/ICS platforms using federated identity or SSO for similar misconfigurations. Review network segmentation controls to confirm ICS-facing applications are not directly internet-accessible. Update asset inventory to track OPTIMAX version and patch status on a recurring basis.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST CM-8 (System Component Inventory), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Conduct a tabletop exercise specifically scoped to: 'What is our detection and response time if an ICS application SSO integration silently fails open?' — this gap was the root condition in CVE-2025-14510. For asset inventory, maintain a spreadsheet or osquery scheduled query tracking all OPTIMAX instances: 'SELECT name, version, install_location FROM programs WHERE name LIKE "%OPTIMAX%";' — schedule this query weekly and alert on any version not equal to 6.3.1-251120 or 6.4.1-251120. For the broader SSO audit, enumerate all OT/ICS applications registered in Azure AD (Entra ID > Enterprise Applications > filter by 'OT' or 'ICS' or 'SCADA' naming convention) and verify each enforces Conditional Access policies requiring compliant devices and MFA.

Evidence: For the post-incident review, compile: (1) The full timeline of OPTIMAX exposure — from when the vulnerable version was deployed to when containment was confirmed — to calculate dwell time and regulatory reporting obligations. (2) The list of all Azure AD enterprise application registrations for OT/ICS systems reviewed in the SSO audit, with their Conditional Access policy status documented. (3) Network topology evidence (firewall rule

exports, network diagram) demonstrating OPTIMAX is no longer internet-reachable, for retention in the incident record and potential regulatory documentation.

Detection Guidance

No public exploit code or active IOCs are currently associated with CVE-2025-14510. Detection should focus on behavioral and log-based indicators: (1) Azure AD sign-in logs, look for OPTIMAX application sign-in events where the SSO token grant is absent or malformed but access was recorded as successful; (2) OPTIMAX application access logs, identify sessions authenticated without a corresponding valid Azure AD token exchange; (3) network monitoring, flag inbound connections to OPTIMAX management interfaces from IPs outside approved ranges, particularly from external addresses; (4) ICS/SCADA integration points, monitor for unexpected configuration reads or writes downstream of OPTIMAX following unauthenticated access. Because exploitation requires no credentials, traditional failed-login alerting will not fire. Focus on access-without-authentication anomalies rather than credential stuffing patterns.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1556** — Modify Authentication Process
- **T1133** — External Remote Services
- **T1199** — Trusted Relationship

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **SI-4** — System Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1556	Modify Authentication Process	Credential-Access
T1133	External Remote Services	Persistence
T1199	Trusted Relationship	Initial-Access

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-04	T1
	https://new.abb.com/news/detail/123639/abb-at-arc-2025-ai-based-sol...	T3
CVE-2025-14510 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-14510	T1
CVE-2025-14510 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2025-14510	T3
CVE-2025-14510 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2025-14510	T3

Generated 2026-04-30 14:09 UTC by TJS Security Command Center