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

ABB Edgenius Management Portal Auth Bypass Enables Remote Code Execution in OT Environments

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0104
Type	CVE Vulnerability
CVE ID	CVE-2025-10571
Severity	HIGH
CVSS Base Score	7.5
Affected Products	ABB Edgenius Management Portal versions 3.2.0.0 and 3.2.1.1
Published	2026-04-30T12:00:00+00:00
Discovery Source	Rss:T2 Gov

Executive Summary

A high-severity authentication bypass flaw in ABB Edgenius Management Portal versions 3.2.0.0 and 3.2.1.1 allows an unauthenticated attacker on the same network to execute arbitrary code, alter configurations, and remove software without any credentials. The product sits at the edge layer of ABB's DCS-to-cloud architecture, meaning exploitation could propagate from the local component into broader operational technology networks across critical manufacturing and industrial control system environments. A patch is available; organizations running affected versions in ICS or OT environments should treat this as a priority remediation.

Technical Analysis

CVE-2025-10571 is an authentication bypass via alternate path or channel (CWE-288) affecting ABB Edgenius Management Portal versions 3.2.0.0 and 3.2.1.1. The vulnerability is network-adjacent exploitable with no authentication required and no user interaction. Successful exploitation grants an attacker arbitrary code execution, application configuration modification, and software uninstall capability on the affected host. CVSS score reporting varies across sources: NVD publishes 7.5 (network-adjacent, no auth required), while CISA ICS advisory context may reference 9.6 for OT impact severity. Verify the authoritative score against the current NVD and CISA entries before operationalizing in risk scoring systems. For OT environments, escalate to risk and compliance teams for context-specific severity reassessment. MITRE ATT&CK techniques mapped to this vulnerability include T1078 (Valid Accounts), T1190 (Exploit Public-Facing Application), T1562.001 (Impair

Defenses: Disable or Modify Tools), T1210 (Exploitation of Remote Services), T1565 (Data Manipulation), and T1059 (Command and Scripting Interpreter). The remediation path is upgrade to ABB Ability Edgenius version 3.2.2.0. No known threat actor exploitation or CISA KEV listing is recorded at this time.

Action Checklist

1. Step 1: Containment, Identify all ABB Edgenius Management Portal instances running versions 3.2.0.0 or 3.2.1.1. Immediately restrict network-adjacent access to the management portal using firewall ACLs or network segmentation controls. Consult the CISA ICS advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-03 for vendor-confirmed network isolation guidance before broader action.
2. Step 2: Detection, Review host-level logs on Edgenius portal systems for unauthenticated session activity, unexpected process executions, configuration file modifications, and software uninstall events. In the OT network, inspect east-west traffic from the Edgenius host for anomalous lateral movement patterns consistent with T1210 or T1059. Absence of authentication log entries preceding configuration changes is a strong signal of exploitation.
3. Step 3: Eradication, Upgrade affected installations to ABB Ability Edgenius version 3.2.2.0 per ABB's remediation guidance. Verify the upgrade path in the CISA ICS advisory and ABB's official documentation before applying in production OT environments. Do not assume a configuration-only workaround is sufficient; the vulnerability is in the authentication path itself.
4. Step 4: Recovery, After patching, validate that authentication is enforced on the management portal by testing access with and without credentials. Review system configurations and installed software inventory for unauthorized changes made prior to or during the exposure window. Monitor the Edgenius host and adjacent OT network segments for 30 days post-remediation for residual indicators of compromise.
5. Step 5: Post-Incident, Conduct a network segmentation review for all edge management components sitting between DCS and cloud layers. Assess whether network-adjacent access to management portals is appropriately restricted across the OT environment. Map this gap to NIST SP 800-82 (Guide to ICS Security) controls for access control and boundary protection, and prioritize closure in the next risk assessment cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and OT operations leadership immediately if forensic evidence confirms exploitation occurred (unauthenticated API calls in Edgenius logs, unauthorized configuration changes, or unexpected process execution from the portal service), if any DCS or historian asset shows anomalous traffic originating from the Edgenius host, or if the organization operates critical manufacturing or energy infrastructure subject to NERC CIP, IEC 62443, or sector-specific OT incident reporting obligations that require regulatory notification.

Recovery Notes	After applying ABB Ability Edgenius 3.2.2.0, actively verify authentication enforcement via unauthenticated API probe testing — do not assume the upgrade succeeded without functional validation. Reconstruct a complete inventory of DCS configurations and installed software on affected Edgenius hosts against a pre-exposure baseline to identify any changes made by an attacker leveraging CVE-2025-10571's configuration-alteration and software-removal capabilities. Maintain elevated monitoring on the Edgenius host and all adjacent OT network segments for 30 days, specifically watching for T1210 (Exploitation of Remote Services) and T1059 (Command and Scripting Interpreter) patterns that would indicate a threat actor established persistence or moved laterally into DCS-layer assets before containment.
Forensic Artifacts	ABB Edgenius application logs (default path: C:\ProgramData\ABB\Edgenius\logs\ — confirm with ABB documentation): search for API requests to configuration management or software package endpoints that lack a preceding valid session authentication entry, which is the direct behavioral signature of CVE-2025-10571 exploitation. | Windows Security Event Log Event ID 4688 (Process Creation) on the Edgenius host: filter for cmd.exe, powershell.exe, wscript.exe, or mshta.exe spawned with a parent process matching the Edgenius portal service — this pattern indicates remote code execution achieved via the auth bypass. | Windows Application Event Log Event IDs 1033 and 1034 (MSI Install/Uninstall) on the Edgenius host: CVE-2025-10571 explicitly enables software removal by unauthenticated attackers, making these events direct evidence of exploitation if they appear during the exposure window without corresponding authorized change records. | Network PCAP or NetFlow from the Edgenius host's OT network interface for the exposure window: look for outbound connections from the Edgenius host to DCS controllers, historians, or engineering workstations on ICS-typical ports (e.g., TCP 102/Modbus, TCP 20000/DNP3, TCP 44818/EtherNet/IP) that would indicate lateral movement from the edge layer into operational technology assets. | Windows Registry hive HKLM\SOFTWARE\ABB\Edgenius and HKLM\SYSTEM\CurrentControlSet\Services: capture and compare against a known-good baseline to detect persistence mechanisms (new services, modified service binaries, or altered configuration registry values) installed by an attacker after gaining unauthenticated code execution access.

Per-Action IR Details

Step 1: Containment — Identify all ABB Edgenius Management Portal instances running versions 3.2.0.0 or 3.2.1.1. Immediately restrict network-adjacent access to the management portal using firewall ACLs or network segmentation controls. Consult the CISA ICS advisory at https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-03 for vendor-confirmed network isolation guidance before broader action.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy; RS.MA-01 (Incident Response Plan Execution)

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Use nmap from a jump host on the OT management VLAN to enumerate hosts with the Edgenius portal's default port open (typically TCP 443 or TCP 8443 — confirm from ABB documentation): 'nmap -p 443,8443 --open -sV '. On the Edgenius host itself, add an inbound Windows Firewall rule via PowerShell to block all non-approved source IPs: 'New-NetFirewallRule -DisplayName "Edgenius-Isolation" -Direction Inbound -LocalPort 443,8443 -Protocol TCP -RemoteAddress -Action Block'. If network infrastructure allows, create an ACL on the adjacent switch or router to drop traffic to the portal from any host outside the dedicated OT admin VLAN.

Evidence: Before isolating, capture a full netstat snapshot from the Edgenius host ('netstat -anob > edgenius_netstat_preiso.txt') to document any active unauthenticated sessions already in progress. Pull the Edgenius application access log (default location varies by ABB install path — check 'C:\ProgramData\ABB\Edgenius\logs\' or

the configured log directory) to preserve a timestamped baseline of all recent connection attempts, including source IPs that established sessions without a preceding authentication event. This pre-isolation evidence window is critical because containment action will terminate active attacker sessions and may destroy in-memory artifacts.

Step 2: Detection — Review host-level logs on Edgenius portal systems for unauthenticated session activity, unexpected process executions, configuration file modifications, and software uninstall events. In the OT network, inspect east-west traffic from the Edgenius host for anomalous lateral movement patterns consistent with T1210 or T1059. Absence of authentication log entries preceding configuration changes is a strong indicator of exploitation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis; DE.AE-02 (Adverse Event Analysis); DE.AE-03 (Information Correlation from Multiple Sources)

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon on the Edgenius host using a config that captures Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Value Set). Query for processes spawned by the Edgenius portal service account using: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 1 -and $_.Message -like '"*edgenius*"}'. For unauthenticated session detection, parse the Edgenius application log for API calls to configuration or software management endpoints that are not preceded by a valid session token entry within the same log sequence. Use Wireshark or tcpdump on the OT network segment to capture east-west traffic from the Edgenius host: 'tcpdump -i -w edgenius_lateral.pcap src host ' — filter for T1210-consistent port scanning or T1059-consistent command-and-control beaconing patterns in the capture.

Evidence: Collect the Edgenius application access and error logs from the ABB install log directory (e.g., 'C:\ProgramData\ABB\Edgenius\logs\') and preserve with hashes (SHA-256) before any log rotation occurs. Pull Windows Security Event Log Event ID 4688 (Process Creation) filtering on processes with a parent process matching the Edgenius portal service — any cmd.exe, powershell.exe, wscript.exe, or mshta.exe spawned from the portal service process is a high-confidence exploitation indicator. Query Windows Event ID 4697 (Service Installation) and Event ID 7045 (New Service Installed) for persistence mechanisms installed post-exploitation. Check Windows Installer logs (Event ID 1033, 1034 in Application log) for unauthorized software uninstall events, which CVE-2025-10571 specifically enables. On the OT network, capture NetFlow or PCAP from the Edgenius host's network interface for the 72-hour window preceding detection to identify lateral movement toward DCS or historian assets.

Step 3: Eradication — Upgrade affected installations to ABB Ability Edgenius version 3.2.2.0 per ABB's remediation guidance. Verify the upgrade path in the CISA ICS advisory and ABB's official documentation before applying in production OT environments. Do not assume a configuration-only workaround is sufficient; the vulnerability is in the authentication path itself.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication; RS.MA-01 (Incident Response Plan Execution)

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), 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 3.2.2.0 upgrade, generate a SHA-256 hash of the current Edgenius application binaries (e.g., 'Get-FileHash -Algorithm SHA256 -Path "C:\Program Files\ABB\Edgenius*" -Recurse | Export-Csv edgenius_pre_patch_hashes.csv') to establish a pre-patch integrity baseline. After upgrade, regenerate hashes and diff the two CSVs to verify only expected files changed. If the upgrade cannot be applied immediately due to OT change control windows, enforce a host-based firewall deny-all-inbound rule on the Edgenius host as a temporary compensating control — but document this explicitly as a time-limited measure, not a fix, because the authentication bypass is in the application layer and no firewall rule repairs it. Scan the host with ClamAV post-upgrade to detect any web shells or dropped payloads installed during any prior exploitation window.

Evidence: Before executing the upgrade, image or snapshot the Edgenius host's application directory, configuration files (including any DCS-to-cloud connector configuration stored under the ABB install path), and the Windows registry hive 'HKLM\SOFTWARE\ABB\Edgenius' to preserve the compromised state for forensic analysis. Capture the full list of installed software via 'Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName,DisplayVersion > installed_pre_patch.csv' — compare against a known-good baseline to identify any software removed by an attacker exploiting CVE-2025-10571's software-removal capability. Preserve IIS or web server access logs (if Edgenius runs on IIS, check 'C:\inetpub\logs\LogFiles\') for any POST requests to configuration or package management API endpoints made without a valid session cookie.

Step 4: Recovery — After patching, validate that authentication is enforced on the management portal by testing access with and without credentials. Review system configurations and installed software inventory for unauthorized changes made prior to or during the exposure window. Monitor the Edgenius host and adjacent OT network segments for 30 days post-remediation for residual indicators of compromise.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery; CSF [RC] — Execute Recovery Plan, Restore Systems, Verify Integrity

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: Validate authentication enforcement by attempting unauthenticated HTTP/HTTPS requests directly to known Edgenius API endpoints (derived from ABB documentation or observed traffic patterns) using curl: 'curl -v -k https://:/api/config' — a 401 or 403 response confirms authentication is now required; a 200 response indicates patching failed or was incomplete. For configuration integrity verification, diff the current Edgenius configuration files against the pre-exploitation backup using 'fc /b' (Windows) or 'diff' (Linux). Use osquery to establish a continuous integrity check: deploy the 'file_events' table watching the Edgenius config directory to alert on any future unauthorized modifications. For the 30-day monitoring window, run a daily scheduled PowerShell task that exports Edgenius application log entries and Windows Event IDs 4688, 4697, and 7045 to a centralized log share for manual review.

Evidence: Post-patch, collect and hash the updated Edgenius binary and configuration files to establish the new verified baseline, and store these hashes offline for future integrity comparisons. Pull Windows Security Event Log Event ID 4624 (Successful Logon) and Event ID 4648 (Logon with Explicit Credentials) from the Edgenius host for the 30-day monitoring window to confirm that all management portal access is now authenticated. Retain all pre-patch forensic images and log exports for a minimum of 90 days in accordance with NIST AU-11 (Audit Record Retention) to support any future regulatory inquiry or post-incident review related to unauthorized configuration changes in the OT environment.

Step 5: Post-Incident — Conduct a network segmentation review for all edge management components sitting between DCS and cloud layers. Assess whether network-adjacent access to management portals is appropriately restricted across the OT environment. Map this gap to NIST SP 800-82 (Guide to ICS Security) controls for access control and boundary protection, and prioritize closure in the next risk assessment cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity; CSF [GV, ID] — Lessons Learned, Update Policies, Improve Detection

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SC-7 (Boundary Protection), NIST AC-1 (Access Control Policy and Procedures), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Enumerate all hosts in the OT environment that occupy the same DCS-to-cloud edge layer as Edgenius by querying your asset inventory (or running nmap against the OT management VLAN) and flag any management portal or API gateway reachable from more than one network zone without authentication enforcement. Document each finding in a risk register entry referencing CVE-2025-10571 as the incident trigger. For network segmentation assessment without enterprise tools, use a manual zone-to-zone connectivity matrix: for each identified

edge component, test reachability from the plant floor VLAN, the OT management VLAN, the IT DMZ, and the cloud connector VLAN using ping and port scans, and document any unintended paths. Feed results directly into the next scheduled risk assessment as a priority finding mapped to NIST SP 800-82 boundary protection requirements.

Evidence: Archive the complete incident timeline — including initial detection timestamp, containment actions, patch application time, and any evidence of exploitation — as a formal after-action record per NIST IR-8 (Incident Response Plan) requirements. Document whether any unauthorized configuration changes or software removals occurred during the exposure window and whether any DCS or historian assets showed anomalous traffic originating from the Edgenius host during that period; this scope determination is required for any regulatory notification assessment under applicable OT/ICS security frameworks. Preserve all network traffic captures, log exports, and forensic images for the incident record and cross-reference against MITRE ATT&CK for ICS technique T0886 (Remote Services) and T0821 (Modify Controller Tasking) to assess whether post-exploitation activity extended beyond the Edgenius host into DCS-layer assets.

Detection Guidance

On the affected Edgenius portal host, search application and system logs for process execution events or configuration changes that are not preceded by a valid authentication event. Look for unexpected software removal events (Windows Event ID 11707 or equivalent uninstall logs on the target OS) originating from the Edgenius service account or network-adjacent source. In network logs, flag unauthenticated HTTP/S requests to the Edgenius management portal interface that receive 200-series responses rather than 401/403. In the broader OT network, monitor for lateral movement from the Edgenius host IP toward DCS components or other industrial assets, consistent with ATT&CK T1210 (Exploitation of Remote Services). Because EPSS score is 0.0 and no active exploitation is currently recorded, prioritize detection as a baseline hygiene measure rather than an active threat hunt.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1562.001** — Disable or Modify Tools
- **T1210** — Exploitation of Remote Services
- **T1565** — Data Manipulation
- **T1059** — Command and Scripting Interpreter

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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring

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
T1562.001	Disable or Modify Tools	Defense-Evasion
T1210	Exploitation of Remote Services	Lateral-Movement
T1565	Data Manipulation	Impact
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
ICS Advisories	https://www.cisa.gov/news-events/ics-advisories/icsa-26-120-03	T1
	https://new.abb.com/news/detail/112803/dcs-of-the-future-cyber-secu...	T3
CVE-2025-10571 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-10571	T1

Source	URL	Tier
CVE-2025-10571 - Vulnerability Details - OpenCVE	https://app.opencve.io/cve/CVE-2025-10571	T3
CVE-2025-10571 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2025-10571	T3

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