INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:20 UTC

CVE-2026-22679: Weaver E-cology Debug API Turned Remote Command Execution Gateway Before Public Disclosure

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0124
Type	CVE Vulnerability
CVE ID	CVE-2026-22679
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0018 (39th percentile)
Affected Products	Weaver E-cology 10.0 (builds prior to March 12, 2026)
Published	2026-05-04T18:12:57
Discovery Source	Rss

Executive Summary

A high-severity unauthenticated remote code execution vulnerability in Weaver E-cology 10.0 was actively exploited in the wild for roughly two weeks before public disclosure, a window during which affected organizations had no awareness of ongoing attacks. The flaw exposed a debug API endpoint that required no authentication and allowed attackers to execute system commands directly. Organizations running this enterprise collaboration platform should treat patching as an immediate priority, as exploitation requires no credentials and no user interaction.

Technical Analysis

CVE-2026-22679 affects Weaver E-cology 10.0 builds prior to March 12, 2026. The vulnerability originates in an exposed debug API endpoint that accepts unauthenticated user input and routes it to backend RPC and OS command execution functions without validation or access control. Exploitation chains CWE-306 (Missing Authentication for Critical Function), CWE-20 (Improper Input Validation), and CWE-78 (OS Command Injection). The reported CVSS base score is 7.5 (High severity per CVSS v3.1 scale: 7.0-8.9 = High). NVD CVSS vector string is pending publication as of reporting date. The attack vector is network-accessible, requires no authentication, and yields direct OS command execution. EPSS score is 0.00181 (39th percentile) as of reporting date, which likely reflects limited public scoring data rather than low exploitation likelihood given

confirmed in-the-wild activity. Exploitation was first observed approximately five days after the vendor issued a silent patch and approximately 14 days before public disclosure. Observed attacker tooling included the Goby exploitation framework. MITRE techniques observed or plausible include T1190 (Exploit Public-Facing Application), T1059/T1059.001 (Command and Scripting Interpreter: PowerShell), T1082 (System Information Discovery), T1057 (Process Discovery), T1016 (System Network Configuration Discovery), T1105 (Ingress Tool Transfer), T1027 (Obfuscated Files or Information), T1133 (External Remote Services), and T1620 (Reflective Code Loading). The vendor's remediation removes the debug endpoint entirely; no access restriction option is offered as an alternative. CVE is indexed in NVD at https://nvd.nist.gov/vuln/detail/CVE-2026-22679, verify for current CVSS vector string and scoring updates.

Action Checklist

1. Step 1: Containment. Identify all Weaver E-cology 10.0 instances in your environment. Immediately restrict external network access to the application if internet-facing. Prioritize instances with no WAF or IPS in front of them. If patching cannot begin within 24 hours, block access to the debug API endpoint path at the perimeter or via host-based firewall rules as a temporary measure.
2. Step 2: Detection. Review web server and application access logs for requests targeting debug API endpoint paths on E-cology instances. Look for unauthenticated POST or GET requests to internal RPC or debug routes, unexpected process spawning from the E-cology application service account (e.g., cmd.exe, sh, PowerShell child processes), and anomalous outbound connections or file downloads originating from the application server. Goby framework scanning activity may appear in logs as structured probe sequences prior to exploitation. Check for T1082/T1016 reconnaissance patterns (system info and network config queries) executed under the application process context.
3. Step 3: Eradication. Apply the vendor patch issued March 12, 2026, which removes the debug endpoint entirely. Confirm the patched build is installed by verifying the build version post-update. Do not rely on access restriction to the endpoint as a permanent fix; the vendor's remediation strategy is endpoint removal, and partial mitigations may leave residual risk. Check the official Weaver vendor advisory and NVD entry for confirmed patch details as additional information is published.
4. Step 4: Recovery. After patching, verify the debug endpoint no longer responds to unauthenticated requests. Review application process logs for exploitation indicators going back to the silent patch date (March 12, 2026) and at least two weeks prior to public disclosure. Confirm no unauthorized accounts, scheduled tasks, cron jobs, or dropped files remain on the application server. Monitor outbound traffic from the E-cology host for 30 days post-remediation given reported failed-but-attempted persistence activity.
5. Step 5: Post-Incident. This vulnerability exposes two systemic control gaps: silent vendor patching without coordinated disclosure left defenders blind during active exploitation, and exposed debug endpoints represent a recurring class of preventable risk. Conduct an inventory of all internet-facing applications with debug, developer, or test endpoints enabled in production. Establish a vendor notification process that flags silent patches for immediate internal triage. Review your vulnerability management SLA to account for pre-disclosure exploitation scenarios.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership and legal/privacy counsel if web server logs confirm unauthenticated requests to the E-cology debug API endpoint between approximately February 26 and March 12, 2026 (the silent exploitation window), as successful RCE during this period may constitute a reportable breach under applicable data protection regulations (e.g., GDPR 72-hour notification, HIPAA 60-day notification) given E-cology's role as an enterprise collaboration platform likely processing PII or business-sensitive data.
Recovery Notes	Post-patch recovery for CVE-2026-22679 must include explicit verification that the Weaver March 12, 2026 build is installed and that the debug endpoint returns 404 to unauthenticated requests — access restriction alone is insufficient because the vendor's remediation removes the endpoint entirely, and any residual path reachability indicates an incomplete patch application. Given reported failed persistence attempts associated with this exploitation campaign, monitor all outbound connections from the E-cology host for a minimum of 30 days using firewall flow logs or osquery process-socket correlation, specifically watching for low-frequency beaconing patterns on ports 80, 443, or non-standard high ports that may indicate a successfully implanted but dormant backdoor. Rotate all service account credentials and API keys associated with the E-cology application before returning the instance to full production, as the unauthenticated RCE primitive may have been used to harvest credentials from the application's configuration files or memory.
Forensic Artifacts	Weaver E-cology web server access logs (IIS W3C logs at C:\inetpub\logs\LogFiles\W3SVC**.log or Nginx/Apache logs at /var/log/nginx/access.log) — specifically entries showing unauthenticated POST or GET requests to debug or internal RPC API paths, with particular attention to source IPs matching Goby framework scan signatures (rapid sequential multi-path probes from a single IP within a short timeframe) | Windows Security Event ID 4688 (Process Creation) or Sysmon Event ID 1 logs filtered for child processes (cmd.exe, powershell.exe, wscript.exe) spawned by the E-cology application service account or JVM process — direct forensic indicator of successful RCE exploitation via the unauthenticated debug API (MITRE T1059) | File system artifacts in the E-cology web application root directory — specifically any .jsp, .jspx, .aspx, or .php files with creation timestamps during the exploitation window (approximately February 26 – March 12, 2026) that were not present in the original application deployment, indicating a webshell dropped via the RCE primitive | Windows Scheduled Tasks export (schtasks /query /fo LIST /v) and Linux crontab listings (crontab -l, /etc/cron.d/, /var/spool/cron/) with creation timestamps falling in the exploitation window — reflecting attacker persistence attempts reported in association with this campaign | Outbound network flow records or firewall logs from the E-cology host showing connections to external IPs initiated by the application process — particularly DNS resolutions or TCP connections on ports 4444, 8443, or 1337 that would indicate reverse shell or C2 staging following successful exploitation (MITRE T1071)

Per-Action IR Details

Step 1: Containment — Identify all Weaver E-cology 10.0 instances in your environment. Immediately restrict external network access to the application if internet-facing. Prioritize instances with no WAF or IPS in front of them. If patching cannot begin within 24 hours, block access to the debug API endpoint path at the perimeter or via host-based firewall rules as a temporary measure.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — 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 network scan using nmap to identify all hosts with Weaver E-cology's default port (typically TCP 80/443 or 8080) and banner-match for E-cology responses: `nmap -p 80,443,8080 --open -sV --script http-title `. Once identified, apply an immediate host-based block on Windows using netsh: `netsh advfirewall firewall add rule name='Block Ecology Debug API' dir=in action=block protocol=TCP localport=`. On Linux use iptables: `iptables -I INPUT -p tcp --dport -j DROP`. For perimeter blocking without a commercial WAF, deploy ModSecurity (free, open source) in front of E-cology and add a rule denying requests to the debug endpoint URI path.

Evidence: Before isolating, capture a full netstat snapshot from the E-cology server (`netstat -anob` on Windows, `ss -tnp` on Linux) to document all active connections at time of containment. Preserve IIS or Apache/Nginx access logs (default paths: Windows IIS — `C:\inetpub\logs\LogFiles\W3SVC*\*.log`; Linux Nginx — `/var/log/nginx/access.log`) showing any recent requests to the debug API path. If the host is Windows, run `tasklist /svc` and `wmic process get processid,parentprocessid,commandline` to snapshot all running processes before network isolation drops attacker-maintained sessions. These captures establish the pre-containment state required by NIST 800-61r3 §3.3 before any disruptive action.

Step 2: Detection — Review web server and application access logs for requests targeting debug API endpoint paths on E-cology instances. Look for unauthenticated POST or GET requests to internal RPC or debug routes, unexpected process spawning from the E-cology application service account (e.g., cmd.exe, sh, PowerShell child processes), and anomalous outbound connections or file downloads originating from the application server. Goby framework scanning activity may appear in logs as structured probe sequences prior to exploitation. Check for T1082/T1016 reconnaissance patterns (system info and network config queries) executed under the application process context.

NIST Phase: Detection Analysis

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

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

Compensating: Deploy Sysmon (free, Sysinternals) on the E-cology Windows host with a configuration that captures Event ID 1 (Process Create) and Event ID 3 (Network Connection). Filter Sysmon Event ID 1 for ParentImage matching the E-cology service executable (e.g., `ecology.exe` or the Tomcat JVM process) and ChildImage matching `cmd.exe`, `powershell.exe`, or `sh`. Use this PowerShell one-liner to search existing Windows Security logs for suspicious child processes: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -match 'cmd.exe|powershell|sh.exe'} | Select-Object TimeCreated, Message | Export-Csv ecologyProcessAudit.csv`. For web log analysis, use grep to isolate debug endpoint hits: `grep -iE '/(debug|rpc|api/debug|ecology.*debug)' /var/log/nginx/access.log | grep -v '401\|403'`. Deploy the community Sigma rule for T1082 (System Information Discovery) converted to a grep-compatible format against Sysmon XML logs using sigmac (free, SigmaHQ).

Evidence: Collect the following before and during analysis: (1) IIS/Nginx/Apache web server access logs covering at least 30 days prior to public disclosure (back to approximately February 26, 2026) — filter for unauthenticated requests (no session cookie or Authorization header) to any URI path containing 'debug', 'rpc', or E-cology-specific internal API route patterns. (2) Sysmon Event ID 1 logs or Windows Security Event ID 4688 logs showing process lineage from the E-cology service account spawning cmd.exe, powershell.exe, or wscript.exe — these are direct indicators of successful RCE via MITRE T1059 (Command and Scripting Interpreter). (3) Sysmon Event ID 3 (Network Connection) or firewall flow logs showing outbound connections from the E-cology process to external IPs, particularly on ports 80, 443, 4444, or 8443 (common reverse shell or C2 ports), consistent with MITRE T1071 (Application Layer Protocol). (4) Web server access logs showing Goby scanner fingerprints — Goby typically sends structured multi-request probe sequences with consistent User-Agent strings and rapid sequential requests to known vulnerable paths; look for repeated requests from the same source IP within seconds targeting multiple E-cology paths. (5) DNS query logs from the E-cology host for any external resolution requests originating from the application process context, indicative of T1071.004 (DNS C2) or payload staging.

Step 3: Eradication — Apply the vendor patch issued March 12, 2026, which removes the debug endpoint entirely. Confirm the patched build is installed by verifying the build version post-update. Do not rely on access restriction to the endpoint as a permanent fix — the vendor's remediation strategy is endpoint

removal; partial mitigations may leave residual risk. Check the official Weaver vendor advisory and NVD entry for the confirmed patch identifier as additional details are published.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — 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: Before patching, generate a file hash baseline of the E-cology application directory using PowerShell: `Get-ChildItem -Recurse 'C:\Weaver\ecology' | Get-FileHash -Algorithm SHA256 | Export-Csv ecology_baseline_prepatch.csv`. After applying the Weaver March 12, 2026 patch, re-run the same command and diff the output: `Compare-Object (Import-Csv ecology_baseline_prepatch.csv) (Import-Csv ecology_baseline_postpatch.csv) -Property Hash,Path`. Verify the debug endpoint servlet or controller file is absent post-patch (its removal is the vendor's stated remediation). Confirm the patched build version by checking the E-cology admin console version page or examining the build manifest file in the application directory. For integrity verification per NIST SI-7, use sigcheck (Sysinternals, free) to validate digital signatures on updated JAR or DLL files if provided by Weaver.

Evidence: Capture pre-patch forensic state before eradication modifies the system: (1) Full directory listing with timestamps of the E-cology web application root, specifically the directory containing the debug API servlet or endpoint handler — this preserves evidence of any attacker-modified or dropped files in the application directory. (2) Registry snapshot on Windows of the E-cology service entry (`HKLM\SYSTEM\CurrentControlSet\Services\`) and scheduled tasks (`schtasks /query /fo LIST /v > schtasks_prepatch.txt`) to detect any attacker-installed persistence before patching removes context. (3) A memory dump (using ProcDump free from Sysinternals: `procdump -ma ecology_predump.dmp`) of the E-cology application process prior to patching if active exploitation is suspected — this may capture in-memory payloads, decoded commands, or attacker tooling that would be lost after service restart during patching.

Step 4: Recovery — After patching, verify the debug endpoint no longer responds to unauthenticated requests. Review application process logs for any prior exploitation indicators going back to the silent patch date (March 12, 2026) and at least two weeks prior to public disclosure. Confirm no unauthorized accounts, scheduled tasks, cron jobs, or dropped files remain on the application server. Monitor outbound traffic from the E-cology host for 30 days post-remediation given reported failed-but-attempted persistence activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Perform a functional verification of the debug endpoint removal by sending a crafted unauthenticated request to the previously vulnerable path using curl: `curl -v -X POST http://:/ -d 'cmd=whoami'` — a 404 or connection refused response confirms endpoint removal; any 200 or 500 response requires immediate re-escalation. For account audit on Windows, run: `net localgroup administrators` and `Get-LocalUser | Select Name,Enabled,LastLogon | Export-Csv localusers_postpatch.csv` and compare against a known-good baseline. For scheduled task audit: `schtasks /query /fo LIST /v | findstr /i 'ecology\|weaver\|cmd\|powershell'`. For Linux, check cron with: `crontab -l; ls -la /etc/cron.*; cat /var/spool/cron/crontabs/*`. Deploy osquery (free) with a query against `listening_ports` and `process_open_sockets` to detect any backdoor listener left by attacker persistence attempts: `SELECT pid, port, protocol FROM listening_ports WHERE port NOT IN (80, 443, 8080);`.

Evidence: Before restoring full production access, document: (1) Results of the curl-based endpoint verification test as recorded evidence of remediation effectiveness per NIST SI-6. (2) Full account audit export (`net localgroup administrators`, AD query if domain-joined) timestamped post-patch to establish a clean-state baseline for any future comparison. (3) Output of a file system scan of the E-cology web root and temp directories for webshells — use ClamAV (free) with the default webshell signatures: `clamscan -r /path/to/ecology/webroot --log=webshell_scan.log` — webshells dropped via this RCE vulnerability would typically reside in the application's publicly accessible directories

with .jsp, .aspx, or .php extensions. (4) Netflow or firewall log exports covering the 30-day monitoring window, segmented by source process if using host-based firewall logging, to support retrospective analysis if C2 beaconing is later identified.

Step 5: Post-Incident — This vulnerability exposes two systemic control gaps: silent vendor patching without coordinated disclosure left defenders blind during active exploitation, and exposed debug endpoints represent a recurring class of preventable risk. Conduct an inventory of all internet-facing applications with debug, developer, or test endpoints enabled in production. Establish a vendor notification process that flags silent patches for immediate internal triage. Review your vulnerability management SLA to account for pre-disclosure exploitation scenarios.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Build a repeatable debug endpoint discovery process using a free tool: configure a scheduled Nikto scan (`nikto -h -Tuning 1 -output nikto_debug_scan.txt`) against all internet-facing application hosts monthly, filtering output for 'debug', 'test', 'dev', or 'admin' path hits. For silent patch monitoring specific to Weaver and similar enterprise software vendors without a public CVE feed, subscribe to their official update bulletin RSS feed or mailing list and create a manual triage ticket whenever a patch is released without an accompanying security advisory — this operationalizes NIST SI-5 at zero cost. Document the CVE-2026-22679 timeline (exploitation window: ~February 26 to March 12, 2026; disclosure gap: ~2 weeks) as a formal lessons-learned entry in your IR plan per NIST IR-8, and use it to benchmark your vulnerability management SLA against pre-disclosure exploitation risk.

Evidence: For the lessons-learned record required by NIST 800-61r3 §4, retain and archive: (1) All web server access logs from the E-cology host covering the full exploitation window (approximately February 26 – March 12, 2026) as the primary evidence set for retrospective scope determination — these logs establish whether your organization was successfully targeted during the silent exploitation period. (2) Timeline reconstruction document mapping first Goby scan probe (if observed in logs) through last detected exploitation attempt, correlated with the vendor patch date of March 12, 2026 and public disclosure date, to quantify actual exposure duration. (3) Inventory output of all internet-facing applications with debug or developer endpoints, generated as a direct output of the post-incident review, serving as baseline for the recurring control improvement per CIS 7.1.

Detection Guidance

Focus detection on the Weaver E-cology application server logs and host-level process telemetry. Key indicators: (1) Unauthenticated requests to debug or internal RPC API paths in web access logs; look for requests with no session token or authentication header to paths inconsistent with normal user workflows. (2) Child processes spawned by the E-cology application service (e.g., cmd.exe, powershell.exe, /bin/sh, /bin/bash); this is abnormal and warrants immediate investigation. (3) Goby framework signatures in network traffic: Goby performs structured enumeration before exploitation; review IDS/IPS logs for probe sequences against the E-cology host. (4) T1105 indicators: outbound HTTP/HTTPS or SMB connections from the application server to external IPs shortly after suspicious requests, particularly file download activity. (5) T1082/T1016 reconnaissance: system information or network configuration commands executing under the application process account. If SIEM is available, correlate web access log anomalies with process creation events (Sysmon Event ID 1 on Windows; auditd execve on Linux) filtered to the application service account. No confirmed public IOC hashes or IPs are available in the provided source data; treat behavioral indicators as higher confidence than static IOCs at this stage.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Debug API endpoint paths on Weaver E-cology (specific paths not publicly confirmed in available sources)`	Unauthenticated requests to internal debug/RPC API paths are the exploitation entry point — specific path strings not yet confirmed in available T1/T3 sources	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1057** — Process Discovery
- **T1059** — Command and Scripting Interpreter
- **T1620** — Reflective Code Loading
- **T1016** — System Network Configuration Discovery
- **T1027** — Obfuscated Files or Information
- **T1082** — System Information Discovery
- **T1105** — Ingress Tool Transfer
- **T1059.001** — PowerShell
- **T1133** — External Remote Services

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
- **CA-7** — Continuous Monitoring
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

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
T1057	Process Discovery	Discovery
T1059	Command and Scripting Interpreter	Execution
T1620	Reflective Code Loading	Defense-Evasion
T1016	System Network Configuration Discovery	Discovery
T1027	Obfuscated Files or Information	Defense-Evasion
T1082	System Information Discovery	Discovery
T1105	Ingress Tool Transfer	Command-And-Control
T1059.001	PowerShell	Execution
T1133	External Remote Services	Persistence

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/weaver-e-cology-crit...	T3
CVE-2026-22679 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-22679	T1
CVE-2026-22679 | Tenable®	https://www.tenable.com/cve/CVE-2026-22679	T3
CVE-2026-22679: Weaver E-cology Unauthenticated RCE ... - GitHub	https://github.com/keraattin/CVE-2026-22679	T3
CVE-2026-22679 Security Vulnerability Analysis & Exploit Details	https://cve.akaoma.com/cve-2026-22679	T3

Generated 2026-05-05 08:20 UTC by TJS Security Command Center