Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Unauthenticated RCE in Weaver E-cology Actively Exploited

Date of Publication	Admiralty Code	TA Number
May 06, 2026	A1	TA2026121

Summary

First Seen: March 2026
Affected Products: Weaver (Fanwei) E-cology 10.0 (builds before 20260312)
Impact: CVE-2026-22679 is a critical flaw in Weaver E-cology 10.0 that is already being actively exploited, giving attackers a direct path to execute system commands without authentication. The issue arises from an exposed Dubbo RPC debug interface that blindly trusts user input, allowing crafted requests to trigger command execution and return results instantly. Threat actors have quickly operationalized the vulnerability, evolving from simple verification attempts to more advanced payload delivery and stealthy, fileless PowerShell execution on compromised systems. With public exploit code and detection tools now available, unpatched deployments are highly exposed and at immediate risk of full system compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-22679	Weaver (Fanwei) E-cology Remote Code Execution Vulnerability	Weaver (Fanwei) E-cology 10.0 versions prior to 20260312	✗	✗	✓

Vulnerability Details

#1

CVE-2026-22679 is a critical unauthenticated remote code execution flaw affecting Weaver (Fanwei) E-cology 10.0, an enterprise collaboration platform. Tracked under CWE-306 (Missing Authentication for Critical Function), the issue stems from a Dubbo RPC debug interface that was inadvertently exposed in production without any authentication or access control. The vulnerable endpoint accepts JSON parameters, interfaceName and methodName, and passes them directly to the RPC invoker, which maps them to backend helper functions capable of executing system-level commands. Because there is no input validation or sanitization, attacker-supplied input is executed directly on the underlying operating system.

#2

Exploitation is straightforward and requires no prior access. An attacker can send a crafted POST request to the exposed endpoint, specifying a known command-execution interface and method. The Dubbo framework processes the request and runs the supplied system command, returning the output in the HTTP response. This creates a direct, synchronous command execution channel without the need for a reverse shell. Observed activity shows that all malicious processes are spawned via java.exe, the JVM instance running under the Tomcat server, confirming that execution occurs within the application context.

#3

The vulnerability impacts all E-cology 10.0 versions released before March 12, 2026. Exploitation in the wild began almost immediately after the patch was issued. Initial activity was observed as early as March 17, followed by broader scanning and exploitation reported later in the month. One documented intrusion demonstrated a staged attack chain on a Windows host, beginning with simple command execution checks, followed by multiple attempts to deploy payloads, and eventually shifting to fileless techniques using PowerShell executed through a renamed binary to evade detection.

#4

Public proof-of-concept and detection tooling are now available, including a Python-based scanner published on GitHub. Given the ease of exploitation and confirmed in-the-wild abuse, organizations using affected versions should urgently upgrade to the patched release and restrict access to exposed interfaces to reduce the risk of compromise.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-22679	Weaver (Fanwei) E-cology 10.0 (Before 20260312)	cpe:2.3:a:weaver:e-cology:*:*:*:*:*:*:*:*	CWE-306

Recommendations

Apply the Vendor Patch Immediately: Update all Weaver E-cology 10.0 instances to build 20260312 or later without delay. The vendor patch shipped on March 12, 2026 and completely removes the vulnerable debug endpoint from the application. Given confirmed active exploitation dating back to March 17, 2026, unpatched instances are at immediate risk of compromise. Coordinate with your Weaver vendor representative or download the update from the official Weaver security download page.

Restrict Network Access to the Vulnerable Endpoint: If immediate patching is not feasible, implement emergency network-level controls to block external access to the `/papi/esearch/data/devops/dubboApi/debug/method` endpoint. Configure web application firewalls (WAF), reverse proxy rules, or network ACLs to deny all inbound traffic to this path. This should be treated as a temporary mitigation only, as internal network attackers or compromised hosts could still reach the endpoint.

Conduct Compromise Assessment on Exposed Instances: For any E-cology instance that was internet-facing prior to patching, perform a thorough compromise assessment. Review web server access logs for POST requests to `/papi/esearch/data/devops/dubboApi/debug/method`. Examine process trees for `java.exe` spawning unexpected child processes such as `cmd.exe`, `powershell.exe`, `ping.exe`, `whoami.exe`, `ipconfig.exe`, or `tasklist.exe`. Search for indicators of compromise including the IP addresses, URLs, file hashes, and filenames documented in the Vega research report.

Implement Network Segmentation for OA Systems: Weaver E-cology instances should not be directly exposed to the public internet. Place OA platforms behind VPN or zero-trust network access (ZTNA) solutions, restrict access to authorized internal users, and segment the network to limit lateral movement in the event of a compromise. This reduces the attack surface for unauthenticated RCE vulnerabilities and limits the blast radius of successful exploitation.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
Defense Evasion	T1036: Masquerading	T1036.003: Rename System Utilities
	T1027: Obfuscated Files or Information	
Command and Control	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Discovery	T1033: System Owner/User Discovery	
	T1016: System Network Configuration Discovery	
	T1057: Process Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	205[.]209[.]116[.]54, 161[.]132[.]49[.]114, 141[.]11[.]89[.]42, 132[.]243[.]172[.]2, 152[.]32[.]173[.]138
URLs	hxxp[:]//205[.]209[.]116[.]54[:]2013/vsgbt[.]exe, hxxp[:]//205[.]209[.]116[.]54[:]2013/hjchhb[.]exe, hxxp[:]//161[.]132[.]49[.]114/config[.]js, hxxp[:]//141[.]11[.]89[.]42/fanwei0324[.]msi, hxxp[:]//132[.]243[.]172[.]2/config/xx[.]ps1, hxxp[:]//132[.]243[.]172[.]2/w-2026/x[.]ps1, hxxp[:]//152[.]32[.]173[.]138/U<16hex>[.]<8hex>
SHA256	147ac3f24b2b63544d65070007888195a98d30e380f2d480edffb3f07a78377f
Filenames	vsgbt.exe, hjchhb.exe, nvm.exe, fanwei0324.msi, 2.txt, xx.ps1, x.ps1

Patch Link

https://www.weaver.com.cn/cs/securityDownload.html#

References

https://blog.vega.io/posts/cve-2026-22679-weaver-ecology-exploitation/

https://www.vulncheck.com/advisories/weaver-e-cology-unauthenticated-rce-via-dubboapi-debug-endpoint

https://ti.qianxin.com/vulnerability/notice-detail/1760

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a demo of **HivePro**.

REPORT GENERATED ON

May 06, 2026 • 11:00 AM

More at www.hivepro.com