Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical PTC Windchill and FlexPLM Deserialization RCE Actively Exploited

Date of Publication	Admiralty Code	TA Number
June 26, 2026	A1	TA2026180

Summary

First Seen: June 17, 2026
Affected Products: PTC Windchill PDMLink, PTC FlexPLM
Impact: CVE-2026-12569 is a critical, unauthenticated remote code execution vulnerability in PTC Windchill PDMLink and FlexPLM, caused by unsafe deserialization of untrusted input. A remote attacker can run arbitrary code over the network without authentication or user interaction, deploying persistent JSP webshells to take control of the server and exfiltrate sensitive engineering and product data. The flaw is being actively exploited in the wild, with no specific threat actor or malware family currently attributed. Given confirmed exploitation and the platform's deep integration into manufacturing and supply-chain environments, affected organizations should prioritize immediate remediation.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-12569	PTC Windchill and FlexPLM Improper Input Validation Vulnerability	PTC Windchill PDMLink, PTC FlexPLM (all Critical Patch Set versions)	✗	✓	✓

Vulnerability Details

#1 PTC Windchill PDMLink and FlexPLM, the product lifecycle management platforms widely deployed across manufacturing, engineering, and retail supply chains, are affected by CVE-2026-12569, a critical remote code execution vulnerability. Successful exploitation allows an attacker to run arbitrary code on a vulnerable server, gaining a foothold within the application and the sensitive engineering and product data it manages.

#2 The root cause lies in the application's failure to validate untrusted input before deserializing it, allowing a crafted object to be processed and executed within the Windchill application context. Because the affected endpoint requires no authentication, an unauthenticated, remote attacker can trigger the flaw by sending a single malicious request over the network, with no user interaction required.

#3 In observed activity, exploitation results in the deployment of persistent JSP webshells into the Windchill login directory, named using sixteen lowercase hexadecimal characters and reached via POST requests that legitimate Windchill traffic never generates. Operators issue commands through a custom X-windchill-req header, whose first character functions as a command selector, and direct compromised hosts to attacker-controlled command-and-control infrastructure for follow-on activity and possible data exfiltration.

#4 The vulnerability impacts Windchill PDMLink and FlexPLM across all Critical Patch Set (CPS) versions, including releases prior to 11.0 M030, with fixed builds released for the 11.0 M030, 11.1 M020, 11.2.1, 12.0.2, 12.1.2, 13.0.2, and 13.1.1 branches. Active exploitation has been confirmed in the wild, with the vendor publishing indicators of compromise including an attacker command-and-control IP address and a webshell file hash, underscoring the urgency of immediate remediation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-12569	PTC Windchill PDMLink and FlexPLM - all CPS (Critical Patch Set) versions, including releases prior to 11.0 M030	cpe:2.3:a:ptc:windchill_pdmlink:*:*:*:*:*:*:*:* cpe:2.3:a:ptc:flexplm:*:*:*:*:*:*:*:*	CWE-20 CWE-502

Recommendations

Apply Vendor Patches Immediately: PTC has released remediation steps and version-specific patches for the affected Windchill and FlexPLM releases. Apply the appropriate patch for your version without delay using the official eSupport article (CS473270), and treat this as an emergency, out-of-cycle update given confirmed active exploitation. For PTC-hosted instances, confirm directly with PTC that remediation has been completed on your behalf.

Hunt for Deployed Webshells: Search the Windchill login directory for JSP files named with a 16-character lowercase hexadecimal pattern, as the attacker names webshells using this convention and new shells may be deployed under different names. Hash-check any suspicious JSP files against the known webshell SHA256, and check for the presence of flst.txt in temporary or Windchill working directories, as its presence confirms attacker file-listing activity. Treat any internet-exposed instance running an affected version as potentially compromised until proven otherwise.

Block Known Attacker Infrastructure: Block the documented command-and-control and indicator IP addresses at the perimeter firewall, prioritizing the primary C2 address. Treat the indicator list as non-exhaustive and continue monitoring, since the vendor notes additional infrastructure may be in use beyond what has been published.

Deploy Detection Rules for Exploitation Activity: Add WAF or IDS rules to block any request containing the custom X-windchill-req header, which has no legitimate use in Windchill, and alert on any HTTP POST to the hex-named JSP webshell pattern under the login path, as legitimate Windchill traffic does not POST to this location. Additionally, alert on large multi-megabyte POST responses originating from JSP files in the Windchill application tier and on the WSDL probe pattern against FlexPLM login JSP resources that precedes exploitation.

Reduce Internet Exposure: Restrict internet exposure of the Windchill and FlexPLM login endpoints wherever operationally feasible, placing the application behind a VPN, reverse proxy, or access controls so that the vulnerable endpoint is not directly reachable from untrusted networks. Reducing attack surface limits exposure to both this vulnerability and future flaws in the same components.

Vulnerability Management: Maintain an accurate inventory of Windchill, FlexPLM, and CPS deployments and their versions, subscribe to PTC's eSupport notifications for ongoing updates on this active situation, and establish a patch cadence that allows rapid emergency deployment for actively exploited, critical vulnerabilities. Evaluate the security posture of internet-facing enterprise applications and third-party platforms on a recurring basis to reduce exposure to high-severity, network-reachable flaws.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
Discovery	T1083: File and Directory Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	5[.]180[.]41[.]35, 216[.]152[.]148[.]54, 172[.]111[.]38[.]31, 104[.]243[.]35[.]131, 74[.]50[.]76[.]146
SHA256	55a1eb4c2d3da04376df39d7ba832569c6af1a37a0cf2b95f754ac898023a30c
Filename	flst.txt

TYPE	VALUE
URLs	/Windchill/login/7c0a0a34c9d8d53b[.]jsp, /Windchill/login/46b158b8607a4c00[.]jsp, /Windchill/login/64652883d9de3299[.]jsp, /Windchill/login/56c9be44a436c4a2[.]jsp, /Windchill/login/4b57d0652345d383[.]jsp, /Windchill/login/ec6ba805a076e709[.]jsp
HTTP Request	X-windchill-req: ?x8Fmgow

Patch Links

https://www.ptc.com/en/support/article/CS473270

https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS473270

References

https://www.ptc.com/en/about/trust-center/advisory-center/active-advisories/windchill-flexplm-rce-vulnerability

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

June 26, 2026 • 09:30 AM

More at www.hivepro.com