Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

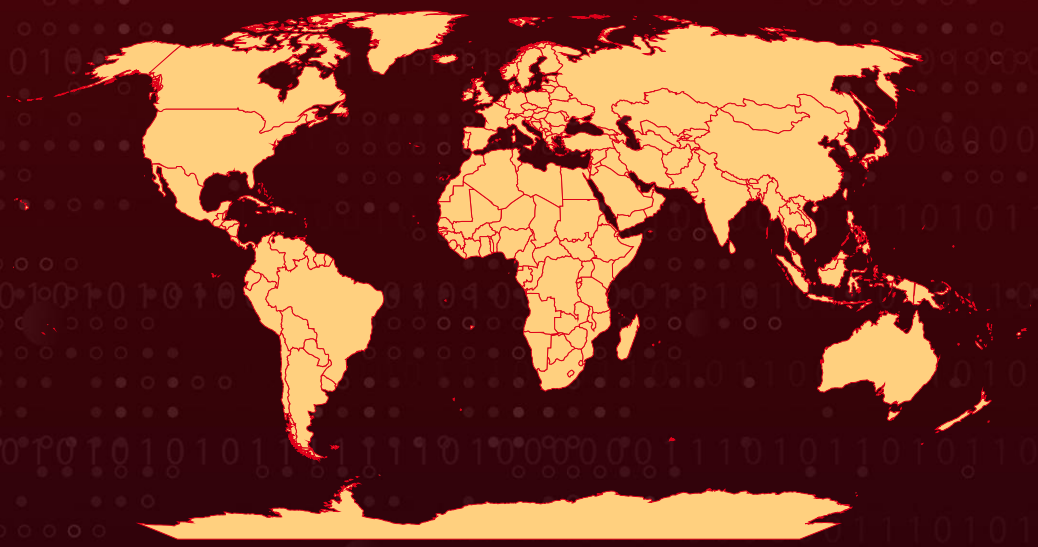
Cl0p-Linked Actors Exploit PTC Windchill and FlexPLM in Data Theft Campaign

Date of Publication	Last Updated Date	Admiralty Code	TA Number
July 28, 2026	August 17, 2026	A2	TA2026214

Summary

First Seen: Early June 2026
Targeted Regions: Worldwide
Targeted Platforms: Java-based application server tier hosting PTC Windchill and FlexPLM
Targeted Products: PTC Windchill PDMLink, PTC FlexPLM
Targeted Industries: Manufacturing, Automotive, Aerospace, Retail, Energy, Financial, Healthcare
Malware: JSP web shell (unnamed)
Threat Actor: Suspected Cl0p affiliate
Attack: Operators suspected of Cl0p affiliation are exploiting internet-exposed PTC Windchill and FlexPLM deployments, chaining a pre-authentication FlexPLM WSDL disclosure with a Windchill login servlet flaw tracked as CVE-2026-12569 for unauthenticated remote code execution, then deploying hex-named JSP web shells and staging engineering and design data for extortion. Extortion emails began 20 July, sent to hundreds of staff from compromised accounts; no encryption stage has been reported, so ransomware-tuned controls will not fire. On or about 12 August the group moved from private extortion to public naming, listing roughly forty plus organisations on its leak site, though the substance of each listing remains attacker-claimed. Attribution remains unconfirmed, resting on tradecraft and branded contact infrastructure. Patches have been available since 17 June, though exploitation may have begun earlier, so retrospective web shell hunting to early June is warranted alongside removal from internet exposure.

Attack Regions



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	✗	✓	✓

Attack Details

#1

An active exploitation campaign is targeting internet-exposed PTC Windchill and FlexPLM Product Lifecycle Management deployments. Operators chain a pre-authentication information disclosure in the FlexPLM WSDL endpoint with a server-side flaw in the Windchill login servlet, tracked as CVE-2026-12569, achieving unauthenticated remote code execution. Neither credentials nor user interaction are required. Affected builds are not confined to older releases, both products are impacted across current version lines, so patch status must be confirmed per build rather than assumed from version age.

#2

Following exploitation, operators write hex-named JSP web shells into the Windchill login directory, establishing remote command execution on the application server. Filesystem enumeration follows, with engineering and design data staged for extortion; the exfiltration channel remains unspecified in current reporting. The confirmed victim sectors remain manufacturing, automotive, aerospace and retail, where PLM platforms hold the intellectual property defining competitive position. The August leak-site listing extends the apparent footprint into energy, financial technology and healthcare technology, though those additions rest on attacker-claimed entries rather than confirmed intrusions.

#3

No encryption stage has been reported. Assessed as data-theft extortion, controls tuned to mass file modification or ransomware execution are unlikely to fire, and an organisation can be fully compromised and its design data removed with no conventional ransomware indicator present. Extortion messaging referencing a serious Windchill PDMLink data leak was first observed on 20 July, sent to hundreds of users within each affected organisation from randomly compromised accounts and carrying the group's latest contact details.

#4 Attribution should remain qualified. The actor behind these intrusions is unconfirmed in available reporting, with the Cl0p association resting on tradecraft consistent with prior campaigns against enterprise applications. Branded extortion mail and leak-site infrastructure establish brand usage rather than identity; suspected Cl0p-affiliated remains the defensible position pending tooling or infrastructure overlap.

#5 PTC patches have been available since 17 June 2026, but patching alone is insufficient. Exploitation is assessed by one source as likely having begun in early June, prior to disclosure, though no published indicator predates 18 June. Retrospective web shell hunting should therefore extend to early June alongside removal of these systems from direct internet exposure. Detection should centre on the Windchill login path, since legitimate traffic does not POST there at all, a higher-fidelity signal than matching web shell filenames, which change between deployments and now span sixteen-character, six-character and dpr_-prefixed naming conventions.

#6 Through late July the group listed no victims and claimed no credit, a silence assessed as characteristic rather than reassuring, matching its pattern across prior file-transfer and ERP campaigns of exploit, exfiltrate, extort privately, then mass-publish. That pattern held. On or about 12 August the group moved to public naming, listing forty plus organisations on its dedicated leak site, detailed in the Recent Breaches section below. The private-to-public transition anticipated at first publication has now occurred; further listings and the release of stolen data are plausible as negotiation windows expire, and victim tracking should continue.

Recommendations

Patch PTC Windchill and FlexPLM: Apply the fixed builds PTC released for CVE-2026-12569, beginning June 17, 2026, across every Windchill PDMLink, FlexPLM and CPS instance. Coverage is not limited to legacy releases: alongside all builds at or below 11.0 M030, specific 11.1, 11.2, 12.x and 13.x builds are individually listed as affected, and the affected build lists differ between Windchill and FlexPLM. Verify each instance against the exact version table in vendor advisory CS473270 rather than inferring status from version age or branch.

Remediate the FlexPLM WSDL Disclosure: Treat the pre-authentication information disclosure in the FlexPLM WSDL endpoint as a separate defect requiring its own fixed build, since patching the Windchill RCE alone leaves one half of the exploitation chain intact.

Track the Second Defect Separately: The FlexPLM WSDL information disclosure carries no assigned CVE and is documented only in the vendor advisory, so it will not appear in CVE-driven patch reporting. Verify its fixed build independently.

Hunt for Hex-Named JSP Webshells: Search the Windchill login directory for files matching /Windchill/login/[0-9a-f]{16}.jsp and compare recovered files against the published SHA-256 hash, treating any unexplained JSP in that path as a compromise indicator.

Alert on the X-windchill-req Header: Configure web server, WAF, and reverse proxy detections for the HTTP request header X-windchill-req: ?x8Fmgow, which is associated with operator interaction with the deployed webshells and has no legitimate application use.

Detect WSDL Reconnaissance Patterns: Build detections for GET requests to /Windchill/rfa/jsp/login/*.jsp?wsdl, giving particular weight to responses of 4045 bytes, to surface pre-exploitation reconnaissance against the FlexPLM WSDL endpoint.

Search for Enumeration Artifacts: Look for a file named flst.txt on Windchill and FlexPLM hosts along with unexplained archives of engineering or design data, both of which indicate filesystem enumeration and staging have already occurred.

Segment the PLM Application Tier: Restrict network paths between the Windchill and FlexPLM application servers and the rest of the environment, including database, directory, and file-share infrastructure, to contain a webshell compromise to the application host.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Resource Development	T1586: Compromise Accounts	T1586.002: Email Accounts
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	
	T1033 : System Owner/User Discovery	
Collection	T1074: Data Staged	T1074.001: Local Data Staging
	T1005: Data from Local System	
	T1560: Archive Collected Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
Impact	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	55a1eb4c2d3da04376df39d7ba832569c6af1a37a0cf2b95f754ac898023a30c
IPv4	216[.]152[.]148[.]54, 216[.]152[.]151[.]204, 104[.]243[.]35[.]63, 5[.]180[.]41[.]35, 23[.]206[.]251[.]247, 38[.]60[.]157[.]212, 64[.]177[.]69[.]57, 64[.]177[.]86[.]200, 65[.]20[.]79[.]73, 66[.]163[.]122[.]78, 74[.]50[.]76[.]146, 78[.]128[.]113[.]10, 79[.]141[.]163[.]103, 81[.]27[.]103[.]18, 81[.]27[.]103[.]68, 85[.]9[.]211[.]83, 87[.]58[.]193[.]42, 104[.]194[.]9[.]14, 104[.]238[.]145[.]147, 104[.]243[.]35[.]0/24, 104[.]243[.]35[.]131, 111[.]194[.]46[.]135, 137[.]184[.]184[.]209, 138[.]68[.]51[.]132, 144[.]172[.]101[.]13, 162[.]243[.]242[.]176, 172[.]111[.]38[.]31, 185[.]227[.]83[.]236, 204[.]194[.]51[.]30, 206[.]189[.]199[.]39, 209[.]222[.]98[.]44, 212[.]147[.]249[.]110, 79[.]141[.]160[.]78

TYPE	VALUE
Filename	flst.txt
File Path	/Windchill/login/[0-9a-f]{16}.jsp, /Windchill/login/dpr_<8 hex>.jsp
HTTP Request	X-windchill-req: ?x8Fmgow, GET /Windchill/rfa/jsp/login/*.jsp?wsdl (response_bytes = 4045)

Recent Breaches

https://www.zebra.com
https://www.netpower.com
https://www.shell.com
https://www.ge.com
https://www.fiserv.com
https://www.philips.com
https://www.aldogroup.com
https://www.irco.com
https://www.toasttab.com
https://www.largan.com.tw
https://www.starkey.com
https://www.partech.com
https://www.mammut.com
https://www.cornelius.com
https://www.mamasandpapas.com
https://www.tristar.com
https://smapcenter.uah.edu
https://www.suunto.cn
https://www.brillonconsumer.com
https://www.jpmgroup.co.in
https://www.clover.com
https://www.atomberg.com
https://www.honghe-tech.com
https://www.intelligentgrowthsolutions.com
https://www.intellihot.com

https://www.9altitudes.com
https://www.waterlandpe.com
https://www.thermos.com
https://www.nuovacmm.com
https://www.ivaluesys.com
https://www.spkaa.com
https://www.lifestraw.com
https://www.omnitanker.com
https://www.archergrey.com
https://www.g3aerospace.com
https://www.itkholding.hu
https://www.midlandind.com.au
https://www.fluidlogic.com
https://www.qcpl.in
https://www.stnet.it
https://www.eccellent.com
https://www.ipmsolutions.sk
https://www.nuvitia.com
https://www.continental.aero
https://www.mindray.com

Patch Links

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

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

References

https://ransom-isac.org/blog/clop-windchill-flexplm-exploitation/

https://www.hivepro.com/threat-advisory/critical-ptc-windchill-and-flexplm-deserialization-rce-actively-exploited

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

July 28, 2026 • 10:45 PM

More at www.hivepro.com