Subject: Immediate Action Required: Notice of Windchill and FlexPLM Critical Vulnerability

PTC has identified a **critical vulnerability (CVSS 10.0)** in its Windchill and FlexPLM products.

This vulnerability could allow remote code execution by an unauthorized party and impacts **all versions of Windchill and FlexPLM**.

You are receiving this message because you are a Windchill and/or FlexPLM customer. **We urge you to take the following remediation steps immediately as patch development is underway.**

Remediation Steps:

- The following Apache HTTP Server configuration update should be IMMEDIATELY applied to every Windchill or FlexPLM system:

  Apache HTTP Server Configuration Remediation Steps:

  1. Create new Apache configuration file

     <APACHE_HOME>/conf/conf.d/**90-app-Windchill-Auth.conf**

  2. Add the following to the body of this new configuration file:

     ```
     <LocationMatch
     "^.*servlet/(WindchillGW|WindchillAuthGW)/com\.ptc\.wvs\.server\.publish\.P
     ublish(?:;[^/]*)?/.*$">
        Require all denied
     </LocationMatch>
     ```

  3. Be sure to save the new configuration file.

NOTES:

- *If there is an Apache HTTP Server configuration file having a sequence number higher than 90, ensure that the new file is the last in the configuration sequence.*

4. Restart the Apache HTTP Server for changes to take effect

   Linux:

   ```
   apachectl stop
   apachectl start
   ```

   Windows (Service):

   Open *Services*
   Stop **Apache HTTP Server**
   Start **Apache HTTP Server**

Indicators of Compromise

In addition to remediation steps outlined above, we urge you to look for the following **indicators of compromise (IOCs)** that can be used to determine if the vulnerability has been exploited in your Windchill or FlexPLM environment:

Network and User-Agent:
Monitor for the following User-Agent Header:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36

Command and Parameter:
Block and/or alert on HTTP requests with suspicious parameters:

- ?c= (command execution)
- ?p= (file read)

File System:
Creation or modification of the following files:

- GW.class
- Gen.class
- Any *.jsp files with a random naming convention that follows this format: “dpr_<8-hex-digits>.jsp”

Check for the presence of any of these files:

- Gen.java – F2C8EB4A4F4BB2344DC0E41C2717B7B0D22F923A1CDBBE61EBF415759F757DAD
- GW.java – 330433BC430CB40E7BC4D17BEBABD521572AD5077F614484FEE9442EEE793477
- HTTPRequest.java – 1CB7A011880958A1A8797D720495646BA8B0601AF09352E4118FCB0E09475E95
- HTTPResponse.java – E697AFEAF83ED975D5B5D2A6604F08E7496D99F9775F33407B0B02530516D88D
- IXBCommonStreamer.java – AFEDA8E680639FE58343AE7A67B92C36E44A67A6BB7DC3C1FC239DF29CF225E0
- IXBStreamer.java – AD388F887F2EB0114AA672EC0D9EE9201916F257EB982C96EC4867727C52082C
- MethodFeedback.java – 305241D4D27B07CFDD566AA16B22CF79116EE9BC254D6D8A8032443ABA2EC985
- MethodResult.java – 69E41E4B68A1097143C394DE25B2E1D33A819AED0C61F3DF891485A98B5AAA07
- WTContextUpdate.java -78473ABBECDFF2BDC30BCB96B0B3EAC3BD6493E6960D11D03277509EFDA188F2

Log and Error IOCs

Unusual error messages in Windchill logs referencing:

- GW_READY_OK
- ClassNotFoundException for GW
- Windchill Error or HTTP Gateway Exception

Customer Support

If you need assistance with the remediation process, please open a technical support case on PTC's eSupport Portal. Effective immediately, PTC is granting 24x7 customer support access and coverage to all PTC customers regardless of support level to address all matters specific to this vulnerability.

If your Windchill or FlexPLM instance is hosted by PTC directly (as opposed to being managed by a PTC partner), we have implemented the above steps for your hosted environment.

We will be communicating further when the patch is finalized.