PTC Security Advisory

This Security Advisory focuses on Server Hardening and Encryption. We encourage you to review carefully the information described in this advisory and strongly recommend that you implement the applicable steps outlined in Section 1 relating to Server Hardening.

Unless otherwise noted, this article covers Windchill Versions 9.x and 10.x

If you have any questions or want to discuss the information contained in this Security Advisory with PTC, you may open a case at support.ptc.com. Those outside of maintenance can file security related issues at the Security Vulnerability Report page found here:
http://support.ptc.com/appserver/support/windchill_security_logger/SecurityLogger.jsp

1 Server Hardening

1.1 This section focuses on hardening the components which comprise the Windchill application against external threats.

1.1.1 Tomcat Communication

PTC is notifying customers who have not yet already done so to take steps now to secure the communication between their Webservers and Embedded or standalone Tomcat in Windchill.

There are two ways to secure this communication. PTC strongly recommends setting up a secret between Apache Webserver and Tomcat as a primary precaution, and a secure firewall as a secondary one. Following both recommendations is also acceptable. These suggestions should not cause any impact to performance. The steps for implementing each of them are set forth below.

Option 1

A secret should be setup between Apache Webserver and Tomcat which would allow only communication from the specific Apache instance to Tomcat. The following instructions will set up this secret. (Note: This option is applicable only to Windchill 8.0 and subsequent versions.)

For PTC HTTP Server:

In <HTTPSERVER_HOME> run the command:

```
ant -DajpRequiredSecret=<secret value> -f config.xml configureAJPWorkers
```

For Embedded Servlet Engine:

For Windchill 10.x, Start in <WT_HOME/tomcat>

For Windchill 8 and 9.x, Start in / <Tomcat_Loadpoint>/

Run the command:

ant -DajpRequiredSecret=<secret value> -f config.xml configureConnectors

In both cases, the <secret value> must be the same string value.

To Setup ANT on a remote/non-PTC supplied Apache Server, please refer to the Installation and Configuration Guide for your Windchill System.
Eg- see page 260 of the M022 10.2 Guide here:
http://support.ptc.com/WCMS/files/163148/en/WCInstallConfigGuide.pdf

Option 2

Option 2 is applicable to all Windchill sites, regardless of version.

If your webserver is located on the same machine as Tomcat, make sure the following AJP Ports are not accessible from outside that machine using local or network firewalls.:

defaults:	8010-8019	Windchill 10.x
	8009-8010	Windchill 6.2.6-9.x

If you are using a remote webserver connecting to the Tomcat from a different machine, configure your firewall to ensure that connections to Tomcat are only allowed from the remote webserver.

As noted above, if there are any questions or comments about these suggestions, you may open a case at support.ptc.com

1.1.2 Suppress Tomcat version information

Similar to the Apache version information as described in later sections, information about the Tomcat version can be misused by an attacker for identifying potential security vulnerabilities.

The procedure to suppress Tomcat version information in error pages is described in PTC Technical Support document: "How to suppress Tomcat version info in error pages."

https://support.ptc.com/appserver/cs/view/case_solution.jsp?n=53391

1.2 Operating System (OS)

In this section, measures to harden the operating system of the server or servers running the Windchill application against attacks and malicious access are addressed.

1.2.1 Deactivation of insecure protocols

Protocols are considered as being “insecure”, if they transfer authentication passwords or content in plain text. The following, non-exhaustive list of “insecure” protocols should be removed and/or deactivated from the Windchill server and not used whenever possible:

telnet: telnetd server daemon listening on port 23

ftp: ftpd server daemon listening on port 21
(Note: CAD Worker Machines may need FTP Servers running)
(Secure FTP (SFTP) available for CAD Workers as of 10.2)

rlogin: rlogind server daemon listening on port 513

rsh: rshd server daemon listening on port 514

IMPORTANT: Prior to their removal or deactivation, verify that the Windchill clients will not require these. Attention should be paid to visualization or CAD worker agents, which might require telnet/ftp to work when configured as remote servers.

1.2.2 Installation of security patches

To harden the server against new security vulnerabilities, it is strongly recommended to keep the Windchill server operating system current by installing the most recent versions of security patches as provided by the OS vendor.

1.3 Apache Web Server

1.3.1 Apache and OpenSSL versions and upgrade

To benefit from security fixes in Apache and OpenSSL it is recommended to always run the most recent version of Apache and OpenSSL provided by PTC through the Apache Early Release Downloads program and Critical Patch Sets

For additional information see “How do I update to a new version of Apache or OpenSSL in Windchill”

https://support.ptc.com/appserver/cs/view/case_solution.jsp?n=174000

1.3.2 Disable directory browsing

By default, Windchill’s Apache configuration allows Apache navigation (~ directory browsing) through the Windows/UNIX file server structure underneath “/Windchill” for any authenticated client. This would allow someone to navigate through the directory structure and compiled code (though password files and other sensitive material is still protected). Therefore, this feature should be deactivated by substituting the “Options FollowSymLinks” entry with “Options –Index –FollowSymLinks” inside Apache base configuration file $APACHE/conf/httpd.conf:

1.3.3 Suppress Apache version information

By default, the Windchill Apache web server provides information about the precise Apache version number as currently installed on the server (e.g. “Server: Apache/2.2.22 (Unix)”). Based on this information, a potential attacker can identify and use a specific security vulnerability exposed by the particular version in question. Therefore, it is strongly recommended to stop the Apache version number from being displayed in any output for the client to see. The following two configurations should be appended to the end of Apache configuration file $APACHE/conf/httpd.conf:

1. ServerSignature: Stop error pages from showing Apache version number

   ServerSignature Off

2. ServerTokens: Stop HTTP header information from including Apache version information

   ServerTokens Prod

Note:

A web server restart is required for these settings to become effective

1.3.4 Disable TRACE HTTP Requests

HTTP Trace Requests can be used for Cross-Site Tracing attacks. Therefore it is recommended to disable the use of HTTP Trace requests within Apache. Append the following line to the end of the Apache configuration file $APACHE/conf/httpd.conf

TraceEnable off

1.3.5 Disable SSLv2 and SSLv3

There are a number of inherent cryptographic flaws in SSL 2.0 and 3.0. Where possible it is recommended to configure Apache to use only TLS for SSL.

Note: The use of a specific SSL protocol on the server will depend on the protocols supported by the clients connecting to the server. Customers should ensure that all their clients support a specific protocol before making any configuration changes in production.

In $APACHE/conf/extra/httpd-ssl.conf add the following line

SSLProtocol All -SSLv2 -SSLv3 +TLSv1

1.3.6 Disable Null and Weak Crytographic Ciphers

Over time, a number of flaws have been found in older cryptographic ciphers and modern computing power that makes it easier to break older ciphers. Therefore, it is recommended to disable Null and weak Ciphers.

In $APACHE/conf/extra/httpd-ssl.conf change the SSLCipherSuite line as follows:

SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

1.3.7 Enable robots.txt

Robots.txt is a standard method for allowing or disallowing web crawling by internet search engines such as Google and Microsoft. This applies to customers with externally accessible systems. While authentication should prevent access by the search engines, this file will tell the crawler to perform no analysis of the system at even the simplest level.

From within the $Apache/htdocs directory create a robots.txt file with the following contents:

```
User-agent: *
Disallow: /
```

This file must be made anonymous to all users.

Encryption

1.4 Data-in-Motion encryption

1.4.1 Configuring Windchill and Apache for HTTPS

This section describes the configuration of Windchill and Apache for HTTPS. The most visible effect of this configuration is the change of the Windchill URL from http://servername/Windchill to https://servername/Windchill.

The HTTPS configuration provides the following two advantages over Windchill's out-of-the-box HTTP deployment:

1. Through the server certificate, the clients can verify the authenticity of the Windchill server to protect against Man-in-the-middle attacks (see Wikipedia Man-in-the-middle attacks article).
2. This configuration provides bidirectional encryption of communications between Windchill client and server to ensure that communication contents cannot be read, forged or tampered with by a third party.

Information on configuring HTTPS can be found as follows

9.1 – The Chapter "Configuring HTTPS for Apache and Windchill" of the "Windchill Installation and Configuration Guide — Advanced" document p190

http://support.ptc.com/WCMS/files/140939/en/WCAdvancedInstallConfigGuide.pdf

10.0 – The Chapter "Configuring HTTPS for Apache and Windchill" of the "Windchill Installation and Configuration Guide" document p166

http://support.ptc.com/WCMS/files/135950/en/WCInstallConfigGuide.pdf

http://support.ptc.com/cs/help/windchill_hc/wc100_hc/index.jspx?id=WCInstall_HTTPSApacheWCConfig&action=show

10.1 – The Chapter “Configuring HTTPS for Apache and Windchill” of the “Windchill Installation and Configuration Guide” document p194

http://support.ptc.com/WCMS/files/137773/en/WCInstallConfigGuide.pdf

http://support.ptc.com/cs/help/windchill_hc/wc101_hc/index.jspx?id=WCInstall_HTTPSApacheWCConfig&action=show

10.2 – The Chapter “Configuring HTTPS for PTC HTTP Server and Windchill” of the “Windchill Installation and Configuration Guide” document p207

http://support.ptc.com/WCMS/files/155680/en/WCInstallConfigGuide.pdf

http://support.ptc.com/cs/help/windchill_hc/wc102_hc/index.jspx?id=WCInstall_HTTPSApacheWCConfig&action=show

General

- “How to configure Windchill to use the https protocol with SSL encryption and (self-signed) certificates in an environment with replica servers”

  https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS166338

- “Configuring Cognos for use with an SSL-enabled Windchill PDMLink server”

  https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS15497

- “How to create self-signed Root and Intermediate SSL certificates for testing in Windchill”

  https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS159762

Note:

- If a self-signed certificate is used, the client has to accept the un-trusted certificate. This can be avoided, if the certificate has previously been installed in the client’s certificate store.
- But this is still an encumbering task to be executed on every new client and user environment. If such a certificate has expired, it has to be replaced everywhere and any errors or omissions can lead to severe downtimes for the client.
- Most enterprise customers have root certificates installed on all their client machines. Such a company’s root certificate normally gets distributed to all clients with the normal installation process of software. The web server certificate then needs to be signed with the company root certificate which is being done by the company’s Certificate Authority CA when creating the server certificate.
- The client has to execute the necessary steps to obtain and manage such a certificate. Also be aware that HTTPS renders the usage of WAN Compressors futile, unless these are also configured with the same certificates.

1.4.2 Encryption of Directory Server/LDAP communication

Encryption of Windchill to the Directory Server communication via LDAP over SSL (also known as LDAPS) is not supported in Windchill 9.1

For Windchill 10.1 +, documentation on setting up Windchill and Apache to use SSL to connect to WindchillDS may be found in chapter "Using SSL to Access the LDAP Server" from the Windchill Directory Server Administrator's Guide

For additional Information see:

"Support information of LDAPS with Windchill PDMLink"

https://support.ptc.com/appserver/cs/view/solution.jsp?n=CS63227

1.5 Data-at-Rest encryption

1.5.1 Master File Vault encryption

PTC recommends locating the Master File Vault in a highly secured and restricted network zone over encrypting the data. This approach ensures retention of an unencrypted copy of the vault content, even in case of issues with key management (e.g. a lost key scenario with encrypted replicas).

1.5.2 Replica content encryption

In cases where Windchill file servers are located in sites not as physically or logically secure as the Master site, PTC recommends to consider encrypting the replica servers at file system (OS) level. Positive results have been obtained by applying Windows Basic file level encryption to the relevant replica file systems.

More detailed information and general advice on Replica security may be found in chapter "Security and Windchill File Servers" from the Windchill Vaulting and Replication Planning document, p. 34.

http://support.ptc.com/WCMS/files/123336/en/WindchillVaultReplication.pdf