Windchill Extension Security Report

Delivery VsCode

Security Level

Approvals and Review	
Approved By	
Date	
Reviewed By	
Review Date	

PTC Approvals and Review	
PTC Product	No
Windchill+	No
FEDRAMP	No
Approved By	
Date	

Details	
Generated	2025/02/13 11:32
Group Id	com.wincomplm
Artifact Id	wex-delivery-files
Name	Delivery VsCode
Version	1.0b1
Beta	Yes
Windchill Version	13.1
Description	Description here
System Extension	No
Approvals	Not set
Generated by	hpan@wincom-plm.com

Security

Details			
CVE Check	N/A	**WVE Check**	N/A
Check Style	N/A	**Obfuscated**	N/A
Isolated codebase	✔	**Sonar**	N/A
Contrast	✔	**Signed**	✔
Jar Signed	✔	**Threat Model**	N/A
PTC Report	N/A		

CVE Suppressions		
ID	**Reason**	**Reference**

Security Information	
Level A	
Offers services to other systems	✔
Server to server with other systems	✔
Browser based communication with other systems	✔
Stores and manages credentials	✔
Any direct database access	✔
Level B	
Escalation privilage access to Windchill	✔
Administration Only UIs	✔
Direct access UIs e.g. downloads	✔
Requires XSS/CSRF testing	✔
Level C	
Implements a Windchill UI	✔

WINCOM

Wincom/PTC Confidential - Results contained in this report should be independently verified, see legal notice.

2

Windchill Vulnerabilities and Exposures

Minimum Level   **B**

Records				
Level B				
ID	**Description**	**File**	**Lines**	**Approved**
WVE-2022-0501	JSP calls backend, possible XSS, CSRF and access issue	compose.jsp	[6]	❌
WVE-2022-0501	JSP calls backend, possible XSS, CSRF and access issue	edkDockerCheck.jsp	[5]	❌
WVE-2022-0501	JSP calls backend, possible XSS, CSRF and access issue	edkUnzipFile.jsp	[5]	❌
WVE-2022-0501	JSP calls backend, possible XSS, CSRF and access issue	runDockerCall.jsp	[4]	❌
WVE-2023-0502	File creation	WexUnzipFiles.java	[15, 35, 41, 46]	❌
WVE-2023-0504	Use of request parameter (XSS risk)	WexCodeServerCommands.java	[32]	❌
WVE-2023-0506	Use of output stream (XSS,Path disclosure risk)	WexCodeServerCommands.java	[40, 52, 54]	❌
WVE-2023-0506	Use of output stream (XSS,Path disclosure risk)	WexMethods.java	[58, 59]	❌

WINCOM

Software Component Analysis (SCA)

Java Libraries				
Group	**Artifact**	**Version**	**Sonar**	**Approved**
com.wincomplm	wt-framework-commons	1.16-13.1	Link	✅

Java Libraries				
Group	**Artifact**	**Version**	**Sonar**	**Approved**

End Points

These represent the external attack surface of the extension and indicates where certain types of testing will be required. Note a false in the OK indicates the End Point has not been reviewed.

JSP End Points							
Name	**Description**	**Params**	**Action**	**OK**	**Admin**	**XSS**	**CSRF**
dockerCaller	dockerCaller.jsp	n/a	n/a	❌			
edkUnzipFile	old\edkUnzipFile.jsp	n/a	n/a	❌			
runDockerCall	runDockerCall.jsp	n/a	n/a	❌			
compose	old\compose.jsp	n/a	n/a	❌			
edkDockerCheck	old\edkDockerCheck.jsp	n/a	n/a	❌			
edkDockerCaller	old\edkDockerCaller.jsp	n/a	n/a	❌			

Rest End Points	
Name	**Description**

Build Configuration

Maven Plugins		
Group	**Artifact**	**Version**
com.wincomplm	maven-build-helpers	1.4
com.wincomplm	wex-audit-doc	1.2
com.wincomplm	wex-builder	1.31
com.wincomplm	wex-obfuscate	1.0
com.wincomplm	wex-security-doc	1.14
com.wincomplm	wex-testplan-doc	1.1
com.wincomplm	wex-windchill-api-scan	1.14
org.apache.maven.plugins	maven-checkstyle-plugin	3.2.1
org.apache.maven.plugins	maven-clean-plugin	3.2.0
org.apache.maven.plugins	maven-compiler-plugin	3.8.1
org.apache.maven.plugins	maven-dependency-plugin	3.2.0
org.apache.maven.plugins	maven-deploy-plugin	3.1.2
org.apache.maven.plugins	maven-help-plugin	3.2.0
org.apache.maven.plugins	maven-install-plugin	3.1.2
org.apache.maven.plugins	maven-jar-plugin	3.2.0
org.apache.maven.plugins	maven-resources-plugin	3.3.1
org.apache.maven.plugins	maven-site-plugin	3.12.1
org.apache.maven.plugins	maven-surefire-plugin	3.2.5
org.codehaus.mojo	build-helper-maven-plugin	3.2.0
org.owasp	dependency-check-maven	11.1.1

Legal Notice

This report has been automatically generated and is provided for informational purposes only. While efforts have been made to ensure the accuracy and reliability of the information contained herein, no guarantee is given regarding its completeness or suitability for any particular purpose.

Wincom Consulting SL disclaim any liability for damages, losses, or consequences arising from the use or reliance upon the information provided herein. The findings and recommendations contained in this report should be independently verified and evaluated by qualified professionals. The recipient agrees to indemnify and hold harmless Wincom Consulting SL from any claims, demands, or actions arising out of or in connection with the use of this report.

WINCOM

Wincom/PTC Confidential - Results contained in this report should be independently verified, see legal notice.

7