Windchill Extension Security Report

Example - File upload

Security Level   C

Approvals and Review	
Approved By	
Date	
Reviewed By	
Review Date	

Details	
Generated	2024/12/08 15:18
Group Id	com.wincomplm
Artifact Id	wex-example-file
Name	Example - File upload
Version	2.0bfalse
Beta	Yes
Windchill Version	13.0
Description	Shows how to upload a file from a UI
System Extension	No
Approvals	Not set
Generated by	simonh@wincom-plm.com

Security

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

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

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

Windchill Vulnerabilities and Exposures

Minimum Level   D

Records				
Level B				
ID	**Description**	**File**	**Lines**	**Approved**
WVE-2022-0501	JSP calls backend, possible XSS, CSRF and access issue	run-diags.jsp	[6]	✅
WVE-2023-0508	Use of Java temp area	Methods.java	[36]	✅

WINCOM

Results contained in this report should be independently verified, see legal notice.

27

Software Component Analysis (SCA)

Java Libraries				
Group	**Artifact**	**Version**	**Sonar**	**Approved**
com.wincomplm	wt-framework-commons	2.0-13.0-SNAPSHOT	Link	✅

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

WINCOM

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**
diags	utils\diags.jsp	n/a	n/a	❌			
run-diags	utils\run-diags.jsp	n/a	n/a	❌			

Rest End Points	
Name	**Description**

Configuration

The configuration options for both Site Admin and Extension Business Configuration

Business Manager Options				
Category	Name	Type	Description	Required

Admin Options				
Category	Name	Type	Description	Required

Build Configuration

Maven Plugins		
Group	**Artifact**	**Version**
com.wincomplm	wex-audit-doc	2.0-SNAPSHOT
com.wincomplm	wex-packager	2.0-SNAPSHOT
com.wincomplm	wex-remapper	2.0-SNAPSHOT
com.wincomplm	wex-security-doc	2.0-SNAPSHOT
com.wincomplm	wex-testplan-doc	2.0-SNAPSHOT
com.wincomplm	wex-windchill-api-scan	2.0-SNAPSHOT
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	3.11.0
org.apache.maven.plugins	maven-deploy-plugin	3.1.1
org.apache.maven.plugins	maven-install-plugin	3.1.1
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	3.2.2
org.owasp	dependency-check-maven	8.4.3

WINCOM

Results contained in this report should be independently verified, see legal notice.

31

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

Results contained in this report should be independently verified, see legal notice.

32