

# Windchill Extension Security Report

Example - Security

The level is between A and D and indicates the potential security risk that this type of code might have.

### Security Level **B** ◀

Wincom Approvals and Review					
Approved By	Simon Heath				
Date	2023-2-20 Approvals are added to the				
Reviewed By	Ellis Douglas	code to show the last time this			
Review Date	2023-2-20	report was reviewed and			
	•	approved			

Details					
Generated	2023/10/26 16:56				
Group Id	com.wincomplm				
Artifact Id	wex-example-security				
Name	Example - Security	All this data is obtained			
Version	1.10	from the meta data of the code			
Beta	No				
Windchill Version	12.1				
Description	Hello to the world of security				
System Extension	No				
Approvals	Not set				
Sonar Link	Link				

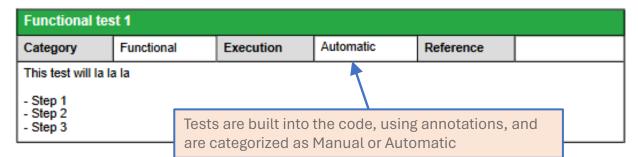
During build the code is sent to the SonarCloud security tool for analysis and the link to the security report is here. We added an example to this report

The report is auto generated on each build; typically during a DevOps pipeline and then stored securely

# Security

Details						
Check Style		<b>O</b>	CVE	<b>O</b>		
Obfuscated		N/A	Isola	Isolated codebase		
SonarQube Enabl	ed	0	Cont	rast Enabled	0	
Signed		0	Jar S	igned	N/A	
Test Plan		0	Wind	chill API Scan	0	
Threat Model		N/A		Various sutameted to	a la can ha	
				Various automated to executed during the k		
CVE Suppresion	IS			COTS and some built		
ID	Reason			analyze Windchill co	ue <u>Neierence</u>	
CVE-2022-45688	This API is encap	psulated and the	re is no att	ack, hutool-json not used	SEC-45	
CVE-2022-26336	poi-scratchpad is	not used	The to	ols can produce false		
negatives. CVEs are checked						
Security Informa	ition		_	st the NIST database a e suppressed	nd	
Level A						
Offers services to oth	ner systems				₩	
Server to server with	other systems				<b>®</b>	
Browser based comr	nunication with o	ther systems			00	
Stores and manages	credentials				89	
Any direct database	access				80	
Level B						
Escalation privilage a	access to Windch	nill			82	
Administration Only I	JIs				00	
Direct access UIs e.g	g. downloads				00	
Requires XSS/CSRF	testing				0	
Level C						
Implements a Windo	hill UI	categories the securit example "A	that will by level on an is not security	must be very well	•	

#### Test Plan



Security	test 1						
Category	Security	Execution	Manual	Reference			
rem aperi Nemo eni	Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem segui nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor						
sit amet, magnam corporis s reprehen fugiat quo	and Selenium for t	he UI. This har a test server. T	opens during th	e xercitatio	labore et dolore onem ullam um iure dolorem eum		

Other test 1						
Category	CUSTOM	Execution	Manual	Reference		
At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique						

at vero eos et accusantos et tusto odio dighissimos ducinius qui bandinis praesentom voluptatum detenti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga. Et harum quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime placeat facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saene eveniet ut et voluptates repudiandae sint et molestiae non recusandae. It reiciendis voluptatibus maiores alias consequatur tracking systems for traceability

Permissions Test					4
Category	Security	Execution	Manual	Reference	SEC-46

The test will evaluate the role-based access control system in place. It will ensure that user roles are clearly defined, and permissions are associated with these roles. In this case, the focus is on the "admin" role and its exclusive access to the UI.

Input Validation							
Category		Security	Execution	Manu	al	Reference	SEC-46
Test that expected Security tests are often developed to test for specific vulnerabilities that are identified by the scanning tools					adheres to		
Request parameter test							

Calling xxx.jsp try to pass an oid that is not accessible by the current user

Execution

Security

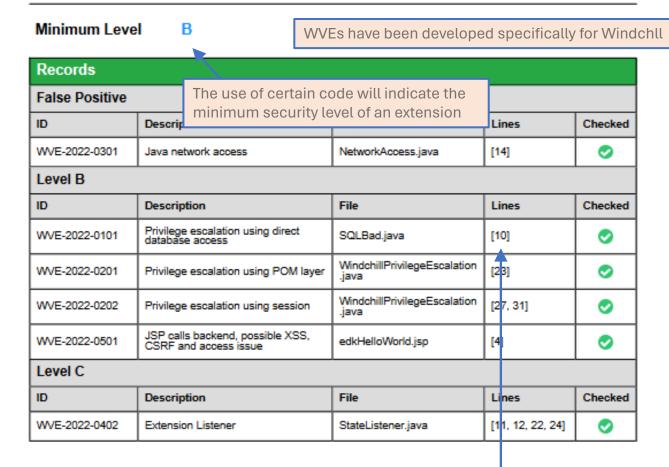
Category

Manual

Reference

SEC-46

## Windchill Vulnerabilities and Explotations



The WVEs indicate the exact position in code of a point of security interest that should be reviewed and many require a test to be developed

Some WVEs may be False Positives and are excluded

The WVE database is reviewed and updated regularly as new threats are detected

Software Component Analysis (SCA)

SCA is an important way to determine which libraries are included in the extension.

Records		are include	ed in the extension.		
Group	Artifact		Version	Sonar	Approved
com.wincomplm	wex-security-doc-annotal	tions	1.1	Link	0
com.zaxxer	SparseBitSet		1.2	7	0
commons-codec	commons-codec		1.15	/	0
commons-io	commons-io		2.11.0		0
org.apache.commons	commons-collections4		4.4		<b>②</b>
org.apache.commons	commons-math3		3.6.1		0
org.apache.logging. log4j	log4j-api		2.18.0		<b>©</b>
org.apache.poi	poi		5.2.3		0

Each custom-built library must be scanned by the security tools. e.g. Sonar

A library can only be included if it is in an approved list.

# **Build Configuration**

Maven Plugins						
Group	Artifact	Version				
com.wincomplm	wex-builder	1.23				
com.wincomplm	wex-security-doc	1.7				
com.wincomplm	wex-windchill-api-scan	1.8				
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	3.10.1				
org.apache.maven.plugins	maven-deploy-plugin	3.1.0				
org.apache.maven.plugins	maven-install-plugin	3.1.0				
org.apache.maven.plugins	maven-jar-plugin	3.2.0				
org.apache.maven.plugins	maven-resources-plugin	3.3.0				
org.apache.maven.plugins	maven-site-plugin	3.12.1				
org.apache.maven.plugins	maven-surefire-plugin	3.0.0				
org.owasp	dependency-check-maven	7.4.4				

The build configuration show what tools were used to build the extension

This includes 3<sup>rd</sup> part COTS security tools

#### Owasp Dependency Report

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

How to read the report | Suppressing false positives | Getting Help: github issues

### Project: wex-example-security

com.wincomplm:wex-example-security:1.10-12.1

Scan Information (show all):

- dependency-check version: 7.4.4
- Report Generated On: Thu, 28 Oct 2023 16:56:22 +0200
- Dependencies Scanned: 8 (8 unique)
- Vulnerable Dependencies: 0
- Vulnerabilities Found: 0
- Vulnerabilities Suppressed: 0
- ٠.
- NVD CVE Checked: 2023-10-26T16:49:47
- NVD CVE Modified: 2023-10-26T16:00:02
- VersionCheckOn: 2023-10-15T16:11:27
- kev.checked: 1698264635

#### Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency Vulnerability IDs Package Highest Severity CVE Count Confidence Evidence Count

### Dependencies

This report contains data retrieved from the National Vulnerability Database.

This report may contain data retrieved from the NPM Public Advisories.

This report may contain data retrieved from RetireJS.

This report may contain data retrieved from the Sonatype OSS Index.

COTS security reports are also included in the report

Other reports can also be appended from the extension

# **Example SonarCloud Report**

