IMPORTANT! Automated tools are an assistant to help to ensure code is secure but do not guarantee secure code.

WINCOM

Windchill Extension Security Report

Example - Security

Security Level B

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

Wincom Approvals and Review	
Approved By	Simon Heath
Date	2023-2-20
Reviewed By	Ellis Douglas
Review Date	2023-2-20

Approvals are added to the code to show the last time this report was reviewed and approved

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

All this data is obtained from the meta data of the code

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	✓	CVE Check	✓
Obfuscated	N/A	Isolated codebase	✓
SonarQube Enabled	✓	Contrast Enabled	✓
Signed	✓	Jar Signed	N/A
Test Plan	✓	Windchill API Scan	✓
Threat Model	N/A		

Various automated tools can be executed during the build. Some are COTS and some built specifically to analyze Windchill code

CVE Suppresions		
ID	Reason	Reference
CVE-2022-45688	This API is encapsulated and there is no attack, hutool-json not used	SEC-45
CVE-2022-26336	poi-scratchpad is not used	

The tools can produce false negatives. CVEs are checked against the NIST database and can be suppressed

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	✓
Level C	
Implements a Windchill UI	✓

Many checks are run and fall into categories that will help to identify the security level of the code. For example “A” is not “bad” but indicates security must be very well checked and tested

Test Plan

Functional test 1

Category	Functional	Execution	Automatic	Reference	

This test will la la la

- Step 1
- Step 2
- Step 3

Tests are built into the code, using annotations, and are categorized as Manual or Automatic

Security test 1

Category	Security	Execution	Manual	Reference	

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 sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, cidunt ut labore et dolore magnam xercitationem ullam corporis tem vel eum iure reprehen illum qui dolorem eum fugiat qu

Automatic tests are run using a combination of Junit and Selenium for the UI. This happens during the build and will use a test server. The code is installed and tested automatically

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 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 saepe eveniet ut et voluptates repudiandae sint et molestiae non recusandae. It us, ut aut reiciendis voluptatibus maiores alias consequatur

We reference back to the issue tracking systems for traceability

Permissions Test

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	Manual	Reference	SEC-46

Test that uest parameters to ensure it adheres to expected

Security tests are often developed to test for specific vulnerabilities that are identified by the scanning tools

Request parameter test

Category	Security	Execution	Manual	Reference	SEC-46

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

Windchill Vulnerabilities and Explotations

Minimum Level B

WVEs have been developed specifically for Windchll

The use of certain code will indicate the minimum security level of an extension

Records

False Positive

ID	Descrip		Lines	Checked
WVE-2022-0301	Java network access	NetworkAccess.java	[14]	✓

Level B

ID	Description	File	Lines	Checked
WVE-2022-0101	Privilege escalation using direct database access	SQLBad.java	[10]	✓
WVE-2022-0201	Privilege escalation using POM layer	WindchillPrivilegeEscalation.java	[23]	✓
WVE-2022-0202	Privilege escalation using session	WindchillPrivilegeEscalation.java	[27, 31]	✓
WVE-2022-0501	JSP calls backend, possible XSS, CSRF and access issue	edkHelloWorld.jsp	[4]	✓

Level C

ID	Description	File	Lines	Checked
WVE-2022-0402	Extension Listener	StateListener.java	[11, 12, 22, 24]	✓

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

Group	Artifact	Version	Sonar	Approved
com.wincomplm	wex-security-doc-annotations	1.1	Link	✓
com.zaxxer	SparseBitSet	1.2		✓
commons-codec	commons-codec	1.15		✓
commons-io	commons-io	2.11.0		✓
org.apache.commons	commons-collections4	4.4		✓
org.apache.commons	commons-math3	3.6.1		✓
org.apache.logging.log4j	log4j-api	2.18.0		✓
org.apache.poi	poi	5.2.3		✓

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 3rd part COTS security tools

Owasp Dependency 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, 26 Oct 2023 16:56:22 +0200
- *Dependencies Scanned*: 8 (8 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 0
- ...
- *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