sonarqube

Project Name	Version	Last Analysis Date
Aspose.Cells for .NET	25.7	2025-07-10

CWE Top 25 (2024) Perspective

CWE Vulnerabilities

0

CWE Rating

A

Categories	🔓 Security Vulnerabilities	
[1] CWE-79 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	0	A
[2] CWE-787 - Out-of-bounds Write	-	
[3] CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0	A
[4] CWE-352 - Cross-Site Request Forgery (CSRF)	0	A
[5] CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	-	
[6] CWE-125 - Out-of-bounds Read	-	
[7] CWE-78 - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0	A
[8] CWE-416 - Use After Free	-	
[9] CWE-862 - Missing Authorization	-	
[10] CWE-434 - Unrestricted Upload of File with Dangerous Type	0	A
[11] CWE-94 - Improper Control of Generation of Code ('Code Injection')	-	
[12] CWE-20 - Improper Input Validation	0	A
[13] CWE-77 - Improper Neutralization of Special Elements used in a Command ('Command Injection')	-	
[14] CWE-287 - Improper Authentication	-	
[15] CWE-269 - Improper Privilege Management	-	

sonarqube

Project Name	Version	Last Analysis Date
Aspose.Cells for .NET	25.7	2025-07-10

CWE Top 25 (2024) Perspective

Categories	Security Vulnerabilities	
[16] CWE-502 - Deserialization of Untrusted Data	0	A
[17] CWE-200 - Information Exposure	0	A
[18] CWE-863 - Incorrect Authorization	-	
[19] CWE-918 - Server-Side Request Forgery (SSRF)	-	
[20] CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer	-	
[21] CWE-476 - NULL Pointer Dereference	0	A
[22] CWE-798 - Use of Hard-coded Credentials	0	A
[23] CWE-190 - Integer Overflow or Wraparound	0	A
[24] CWE-400 - Uncontrolled Resource Consumption	0	A
[25] CWE-306 - Missing Authentication for Critical Function	-	

Security ratings

A	-	no vulnerabilities
B	-	at least one minor vulnerability
C	-	at least one major vulnerability
D	-	at least one critical vulnerability
E	-	at least one blocker vulnerability