Project Name	Version	Last Analysis Date
GroupDocs.Conversion for .NET	26.10	2026-10-30

CWE Top 25 (2025) 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-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	0 A
[3] CWE-352 - Cross-Site Request Forgery (CSRF)	0 A
[4] CWE-862 - Missing Authorization	-
[5] CWE-787 - Out-of-bounds Write	-
[6] CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	-
[7] CWE-416 - Use After Free	-
[8] CWE-125 - Out-of-bounds Read	-
[9] CWE-78 - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	0 A
[10] CWE-94 - Improper Control of Generation of Code ('Code Injection')	0 A
[11] CWE-120 - Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	-
[12] CWE-434 - Unrestricted Upload of File with Dangerous Type	0 A
[13] CWE-476 - NULL Pointer Dereference	-
[14] CWE-121 - Stack-based Buffer Overflow	-

Project Name	Version	Last Analysis Date
GroupDocs.Conversion for .NET	26.10	2026-10-30

CWE Top 25 (2025) Perspective

Categories	Security Vulnerabilities
[15] CWE-502 - Deserialization of Untrusted Data	0 A
[16] CWE-122 - Heap-based Buffer Overflow	-
[17] CWE-863 - Incorrect Authorization	-
[18] CWE-20 - Improper Input Validation	0 A
[19] CWE-284 - Improper Access Control	0 A
[20] CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor	0 A
[21] CWE-306 - Missing Authentication for Critical Function	-
[22] CWE-918 - Server-Side Request Forgery (SSRF)	0 A
[23] CWE-77 - Improper Neutralization of Special Elements used in a Command ('Command Injection')	-
[24] CWE-639 - Authorization Bypass Through User-Controlled Key	-
[25] CWE-770 - Allocation of Resources Without Limits or Throttling	0 A

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