2025 CWE Top 25 Most Dangerous Software Weaknesses

Top 25 Home | Share via: X | View in table format | Key Insights | Methodology

1 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-79 | CVEs in KEV: 7 | Rank Last Year: 1

2 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-89 | CVEs in KEV: 4 | Rank Last Year: 3 (up 1) ▲

3 Cross-Site Request Forgery (CSRF)
CWE-352 | CVEs in KEV: 0 | Rank Last Year: 4 (up 1) ▲

4 Missing Authorization
CWE-862 | CVEs in KEV: 0 | Rank Last Year: 9 (up 5) ▲

5 Out-of-bounds Write
CWE-787 | CVEs in KEV: 12 | Rank Last Year: 2 (down 3) ▼

6 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-22 | CVEs in KEV: 10 | Rank Last Year: 5 (down 1) ▼

7 Use After Free
CWE-416 | CVEs in KEV: 14 | Rank Last Year: 8 (up 1) ▲

8 Out-of-bounds Read
CWE-125 | CVEs in KEV: 3 | Rank Last Year: 6 (down 2) ▼

9 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-78 | CVEs in KEV: 20 | Rank Last Year: 7 (down 2) ▼

10 Improper Control of Generation of Code ('Code Injection')
CWE-94 | CVEs in KEV: 7 | Rank Last Year: 11 (up 1) ▲

11 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-120 | CVEs in KEV: 0 | Rank Last Year: N/A

12 Unrestricted Upload of File with Dangerous Type
CWE-434 | CVEs in KEV: 4 | Rank Last Year: 10 (down 2) ▼

13 NULL Pointer Dereference
CWE-476 | CVEs in KEV: 0 | Rank Last Year: 21 (up 8) ▲

14 Stack-based Buffer Overflow
CWE-121 | CVEs in KEV: 4 | Rank Last Year: N/A

15 Deserialization of Untrusted Data
CWE-502 | CVEs in KEV: 11 | Rank Last Year: 16 (up 1) ▲

16 Heap-based Buffer Overflow
CWE-122 | CVEs in KEV: 6 | Rank Last Year: N/A

17 Incorrect Authorization
CWE-863 | CVEs in KEV: 4 | Rank Last Year: 18 (up 1) ▲

18 Improper Input Validation
CWE-20 | CVEs in KEV: 2 | Rank Last Year: 12 (down 6) ▼

19 Improper Access Control
CWE-284 | CVEs in KEV: 1 | Rank Last Year: N/A

20 Exposure of Sensitive Information to an Unauthorized Actor
CWE-200 | CVEs in KEV: 1 | Rank Last Year: 17 (down 3) ▼

21 Missing Authentication for Critical Function
CWE-306 | CVEs in KEV: 11 | Rank Last Year: 25 (up 4) ▲

22 Server-Side Request Forgery (SSRF)
CWE-918 | CVEs in KEV: 0 | Rank Last Year: 19 (down 3) ▼

23 Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-77 | CVEs in KEV: 2 | Rank Last Year: 13 (down 10) ▼

24 Authorization Bypass Through User-Controlled Key
CWE-639 | CVEs in KEV: 0 | Rank Last Year: 30 (up 6) ▲

25 Allocation of Resources Without Limits or Throttling
CWE-770 | CVEs in KEV: 0 | Rank Last Year: 26 (up 1) ▲