CWE TOP 25 Most Dangerous Software Errors

What Errors Are Included in the Top 25 Software Errors?

Click on the CWE ID in any of the listings in the chart below and you will be directed to the relevant spot in the MITRE CWE site where you will find the following:

- Ranking of each Top 25 entry,
- Links to the full CWE entry data,
- Data fields for weakness prevalence and consequences,
- Remediation cost,
- Ease of detection,
- Code examples,
- Detection Methods,
- Attack frequency and attacker awareness
- Related CWE entries, and
- Related patterns of attack for this weakness.

Each entry at the Top 25 Software Errors site also includes fairly extensive prevention and remediation steps that developers can take to mitigate or eliminate the weakness.

- The New 25 Most Dangerous Programming Errors
- The Scoring System
- The Risk Management System

The CWE Top 25

Name	Rank	ID
Out-of-bounds Write	1	CWE-787 https://cwe.mitre.org/data/definitions/787.html
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	2	CWE-79 https://cwe.mitre.org/data/definitions/79.html
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	3	CWE-89 https://cwe.mitre.org/data/definitions/89.html
Use After Free	4	CWE-416 https://cwe.mitre.org/data/definitions/416.html

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	5	CWE-78 https://cwe.mitre.org/data/definitions/78.html
Improper Input Validation	6	CWE-20 https://cwe.mitre.org/data/definitions/20.html
Out-of-bounds Read	7	CWE-125 https://cwe.mitre.org/data/definitions/125.html
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	8	CWE-22 https://cwe.mitre.org/data/definitions/22.html
Cross-Site Request Forgery (CSRF)	9	CWE-352 https://cwe.mitre.org/data/definitions/352.html
Unrestricted Upload of File with Dangerous Type	10	CWE-434 https://cwe.mitre.org/data/definitions/434.html
Missing Authorization	11	CWE-862 https://cwe.mitre.org/data/definitions/862.html
NULL Pointer Dereference	12	CWE-476 https://cwe.mitre.org/data/definitions/476.html
Improper Authentication	13	CWE-287 https://cwe.mitre.org/data/definitions/287.html
Integer Overflow or Wraparound	14	CWE-190 https://cwe.mitre.org/data/definitions/190.html
Deserialization of Untrusted Data	15	CWE-502 https://cwe.mitre.org/data/definitions/502.html
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16	CWE-77 https://cwe.mitre.org/data/definitions/77.html
Improper Restriction of Operations within the Bounds of a Memory Buffer	17	CWE-119 https://cwe.mitre.org/data/definitions/119.html
Use of Hard-coded Credentials	18	CWE-798 https://cwe.mitre.org/data/definitions/798.html
Server-Side Request Forgery (SSRF)	19	CWE-918 https://cwe.mitre.org/data/definitions/918.html
Missing Authentication for Critical Function	20	CWE-306 https://cwe.mitre.org/data/definitions/306.html
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21	CWE-362 https://cwe.mitre.org/data/definitions/362.html
Improper Privilege Management	22	CWE-269 https://cwe.mitre.org/data/definitions/269.html
Improper Control of Generation of Code ('Code Injection')	23	CWE-94 https://cwe.mitre.org/data/definitions/94.html
Incorrect Authorization	24	CWE-863 https://cwe.mitre.org/data/definitions/863.html
Incorrect Default Permissions	25	CWE-276 https://cwe.mitre.org/data/definitions/276.html

Resources to Help Eliminate The Top 25 Software Errors

1. SANS Application Security Courses

The SANS Cloud Security curriculum seeks to ingrain security into the minds of every developer in the world by providing world-class educational resources to design, develop, procure, deploy, and manage secure software. The SANS cloud security and DevSecOps faculty are real-world practitioners with decades of application security experience. The concepts covered in our courses will be applicable to your software security program the day you return to work:

- SEC522: Application Security: Securing Web Apps, APIs, and Microservices
- SEC540: Cloud Security and DevSecOps Automation

SANS maintains an Application Security CyberTalent Assessment that measures secure coding skills and allow programmers to determine gaps in their knowledge of secure coding and allows buyers to ensure outsourced programmers have sufficient programming skills. Organizations can learn more at https://www.sans.org/cybersecurity-assessments/application-security/

2. Developer Security Awareness Training

The SANS Security Awareness Developer product provides pinpoint software security awareness training on demand, all from the comfort of your desk. Application security awareness training includes over 30+ modules averaging 7-10 minutes in length to maximize learner engagement and retention. The modules cover the full breadth and depth of topics for PCI Section 6.5 compliance and the items that are important for secure software development.

3. The TOP 25 Errors List will be updated regularly and will be posted at both the SANS and MITRE sites

CWE Top 25 Software Errors Site

MITRE maintains the CWE (Common Weakness Enumeration) web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 Software errors along with authoritative guidance for mitigating and avoiding them. That site also contains data on more than 700 additional Software errors, design errors and architecture errors that can lead to exploitable vulnerabilities. CWE Web Site

4. SAFECode

The Software Assurance Forum for Excellence in Code (members include EMC, Juniper, Microsoft, Nokia, SAP and Symantec) has produced two excellent publications outlining industry best practices for software assurance and providing practical advice for implementing proven methods for secure software development.

Fundamental Practices for Secure Software Development 3rd Edition

https://safecode.org/publications/#safecodepublications-2362

Overview of Software Integrity Controls

https://safecode.org/publications/#safecodepublications-189

Framework for Software Supply Chain Integrity

https://safecode.org/publications/#safecodepublications-188

Fundamental Practices for Secure Software Development

https://safecode.org/publications/#safecodepublications-186

Software Assurance: An Overview of Current Industry Best Practices

https://safecode.org/publications/#safecodepublications-185

5. Software Assurance Community Resources Site and DHS web sites

As part of DHS risk mitigation efforts to enable greater resilience of cyber assets, the Software Assurance Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to routinely acquire, develop and deploy reliable and trustworthy software products with predictable execution, and to improve diagnostic capabilities to analyze systems for exploitable weaknesses.

6. Nearly a dozen software companies offer automated tools that test programs for these errors.

How Important Are the Top 25 Software Errors?

“ Just wanted to commend the depth of the CWE/SANS Top 25. The code examples are particularly excellent. I have asked all my developers to read one of these each day for the next 25 days. I'm taking my own advice as

Contributors to the 2021 CWE Top 25:

In alphabetical order: Adam Chaudry, Steve Christey Coley, Kerry Crouse, Kevin Davis, Devon Ellis, Parker Garrison, Christina Johns, Luke Malinowski, Rushi Purohit, Becky Powell, David Rothenberg, Alec Summers, and Brian Vohaska.

Members of the NIST NVD Team that coordinated on the Top 25 include Christopher Turner, Robert Byers, and Vidya Ananthakrishna.