Nature	Type	ID	Name	V	Page
HasMember	B	242	Use of Inherently Dangerous Function	734	593
HasMember	B	272	Least Privilege Violation	734	663
HasMember	B	273	Improper Check for Dropped Privileges	734	667
HasMember	B	363	Race Condition Enabling Link Following	734	904
HasMember	B	366	Race Condition within a Thread	734	910
HasMember	B	562	Return of Stack Variable Address	734	1287
HasMember	C	667	Improper Locking	734	1472
HasMember	V	686	Function Call With Incorrect Argument Type	734	1517
HasMember	C	696	Incorrect Behavior Order	734	1535

Notes

Relationship

In the 2008 version of the CERT C Secure Coding standard, the following rules were mapped to the following CWE IDs: CWE-59 POS01-C Check for the existence of links when dealing with files CWE-170 POS30-C Use the readlink() function properly CWE-242 POS33-C Do not use vfork() CWE-272 POS02-C Follow the principle of least privilege CWE-273 POS37-C Ensure that privilege relinquishment is successful CWE-363 POS35-C Avoid race conditions while checking for the existence of a symbolic link CWE-366 POS00-C Avoid race conditions with multiple threads CWE-562 POS34-C Do not call putenv() with a pointer to an automatic variable as the argument CWE-667 POS31-C Do not unlock or destroy another thread's mutex CWE-686 POS34-C Do not call putenv() with a pointer to an automatic variable as the argument CWE-696 POS36-C Observe correct revocation order while relinquishing privileges

References

[REF-597]Robert C. Seacord. "The CERT C Secure Coding Standard". 1st Edition. 2008 October 4. Addison-Wesley Professional.

Category-751: 2009 Top 25 - Insecure Interaction Between Components

Category ID : 751

Summary

Weaknesses in this category are listed in the "Insecure Interaction Between Components" section of the 2009 CWE/SANS Top 25 Programming Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	750	Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors	750	2583
HasMember	C	20	Improper Input Validation	750	20
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	750	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	750	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	750	206
HasMember	C	116	Improper Encoding or Escaping of Output	750	287
HasMember	B	209	Generation of Error Message Containing Sensitive Information	750	540
HasMember	B	319	Cleartext Transmission of Sensitive Information	750	786
HasMember	B	352	Cross-Site Request Forgery (CSRF)	750	875

Nature	Type	ID	Name	V	Page
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	750	895

References

[REF-615]"2009 CWE/SANS Top 25 Most Dangerous Programming Errors". 2009 January 2. < https://cwe.mitre.org/top25/archive/2009/2009_cwe_sans_top25.html >.2024-11-17.

Category-752: 2009 Top 25 - Risky Resource Management

Category ID : 752

Summary

Weaknesses in this category are listed in the "Risky Resource Management" section of the 2009 CWE/SANS Top 25 Programming Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	750	Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors	750	2583
HasMember	B	73	External Control of File Name or Path	750	133
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	750	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	750	299
HasMember	C	404	Improper Resource Shutdown or Release	750	987
HasMember	B	426	Untrusted Search Path	750	1035
HasMember	B	494	Download of Code Without Integrity Check	750	1192
HasMember	C	642	External Control of Critical State Data	750	1422
HasMember	C	665	Improper Initialization	750	1465
HasMember	P	682	Incorrect Calculation	750	1507

References

[REF-615]"2009 CWE/SANS Top 25 Most Dangerous Programming Errors". 2009 January 2. < https://cwe.mitre.org/top25/archive/2009/2009_cwe_sans_top25.html >.2024-11-17.

Category-753: 2009 Top 25 - Porous Defenses

Category ID : 753

Summary

Weaknesses in this category are listed in the "Porous Defenses" section of the 2009 CWE/SANS Top 25 Programming Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	750	Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors	750	2583
HasMember	B	250	Execution with Unnecessary Privileges	750	606
HasMember	V	259	Use of Hard-coded Password	750	630
HasMember	C	285	Improper Authorization	750	691

Nature	Type	ID	Name	V	Page
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	750	806
HasMember	C	330	Use of Insufficiently Random Values	750	821
HasMember	C	602	Client-Side Enforcement of Server-Side Security	750	1359
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	750	1559
HasMember	B	798	Use of Hard-coded Credentials	750	1699

References

[REF-615]"2009 CWE/SANS Top 25 Most Dangerous Programming Errors". 2009 January 2. < https://cwe.mitre.org/top25/archive/2009/2009_cwe_sans_top25.html >.2024-11-17.

Category-801: 2010 Top 25 - Insecure Interaction Between Components

Category ID : 801

Summary

Weaknesses in this category are listed in the "Insecure Interaction Between Components" section of the 2010 CWE/SANS Top 25 Programming Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	800	Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors	800	2584
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	800	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	800	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	800	206
HasMember	B	209	Generation of Error Message Containing Sensitive Information	800	540
HasMember	F	352	Cross-Site Request Forgery (CSRF)	800	875
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	800	895
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	800	1055
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	800	1353

References

[REF-732]"2010 CWE/SANS Top 25 Most Dangerous Software Errors". 2010 February 4. < https://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.html >.2024-11-17.

Category-802: 2010 Top 25 - Risky Resource Management

Category ID : 802

Summary

Weaknesses in this category are listed in the "Risky Resource Management" section of the 2010 CWE/SANS Top 25 Programming Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	800	Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors	800	2584
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	800	33
HasMember	V	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	800	242
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	800	310
HasMember	V	129	Improper Validation of Array Index	800	347
HasMember	B	131	Incorrect Calculation of Buffer Size	800	361
HasMember	B	190	Integer Overflow or Wraparound	800	478
HasMember	B	494	Download of Code Without Integrity Check	800	1192
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	800	1577
HasMember	B	770	Allocation of Resources Without Limits or Throttling	800	1622
HasMember	B	805	Buffer Access with Incorrect Length Value	800	1711

References

[REF-732]"2010 CWE/SANS Top 25 Most Dangerous Software Errors". 2010 February 4. < https://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.html >.2024-11-17.

Category-803: 2010 Top 25 - Porous Defenses

Category ID : 803

Summary

Weaknesses in this category are listed in the "Porous Defenses" section of the 2010 CWE/SANS Top 25 Programming Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	800	Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors	800	2584
HasMember	C	285	Improper Authorization	800	691
HasMember	B	306	Missing Authentication for Critical Function	800	748
HasMember	C	311	Missing Encryption of Sensitive Data	800	764
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	800	806
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	800	1559
HasMember	B	798	Use of Hard-coded Credentials	800	1699
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	800	1723

References

[REF-732]"2010 CWE/SANS Top 25 Most Dangerous Software Errors". 2010 February 4. < https://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.html >.2024-11-17.

Category-808: 2010 Top 25 - Weaknesses On the Cusp

Category ID : 808

Summary

Weaknesses in this category are not part of the general Top 25, but they were part of the original nominee list from which the Top 25 was drawn.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	800	Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors	800	2584
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	800	112
HasMember	B	134	Use of Externally-Controlled Format String	800	371
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	800	551
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	800	754
HasMember	C	330	Use of Insufficiently Random Values	800	821
HasMember	V	416	Use After Free	800	1019
HasMember	B	426	Untrusted Search Path	800	1035
HasMember	B	454	External Initialization of Trusted Variables or Data Stores	800	1092
HasMember	V	456	Missing Initialization of a Variable	800	1096
HasMember	B	476	NULL Pointer Dereference	800	1139
HasMember	C	672	Operation on a Resource after Expiration or Release	800	1488
HasMember	B	681	Incorrect Conversion between Numeric Types	800	1504
HasMember	B	749	Exposed Dangerous Method or Function	800	1572
HasMember	B	772	Missing Release of Resource after Effective Lifetime	800	1632
HasMember	C	799	Improper Control of Interaction Frequency	800	1708
HasMember	B	804	Guessable CAPTCHA	800	1710

References

[REF-732]"2010 CWE/SANS Top 25 Most Dangerous Software Errors". 2010 February 4. < https://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.html >.2024-11-17.

Category-810: OWASP Top Ten 2010 Category A1 - Injection

Category ID : 810

Summary

Weaknesses in this category are related to the A1 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	809	155
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	809	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	809	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	809	217

Nature	Type	ID	Name	V	Page
HasMember	B	91	XML Injection (aka Blind XPath Injection)	809	220

References

[REF-761]OWASP. "Top 10 2010-A1-Injection". < http://www.owasp.org/index.php/Top_10_2010-A1-Injection >.

Category-811: OWASP Top Ten 2010 Category A2 - Cross-Site Scripting (XSS)

Category ID : 811

Summary

Weaknesses in this category are related to the A2 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	809	168

References

[REF-762]OWASP. "Top 10 2010-A2-Cross-Site Scripting (XSS)". < http://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_%28XSS%29 >.

Category-812: OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management

Category ID : 812

Summary

Weaknesses in this category are related to the A3 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	C	287	Improper Authentication	809	699
HasMember	B	306	Missing Authentication for Critical Function	809	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	809	754
HasMember	B	798	Use of Hard-coded Credentials	809	1699

References

[REF-763]OWASP. "Top 10 2010-A3-Broken Authentication and Session Management". < http://www.owasp.org/index.php/Top_10_2010-A3-Broken_Authentication_and_Session_Management >.

Category-813: OWASP Top Ten 2010 Category A4 - Insecure Direct Object References

Category ID : 813

Summary

Weaknesses in this category are related to the A4 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	809	33
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	809	249
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	809	1055
HasMember	B	639	Authorization Bypass Through User-Controlled Key	809	1415
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	809	1750
HasMember	C	862	Missing Authorization	809	1789
HasMember	C	863	Incorrect Authorization	809	1796

References

[REF-764]OWASP. "Top 10 2010-A4-Insecure Direct Object References". < http://www.owasp.org/index.php/Top_10_2010-A4-Insecure_Direct_Object_References >.

Category-814: OWASP Top Ten 2010 Category A5 - Cross-Site Request Forgery(CSRF)

Category ID : 814

Summary

Weaknesses in this category are related to the A5 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember		352	Cross-Site Request Forgery (CSRF)	809	875

References

[REF-765]OWASP. "Top 10 2010-A5-Cross-Site Request Forgery (CSRF)". < http://www.owasp.org/index.php/Top_10_2010-A5-Cross-Site_Request_Forgery_%28CSRF%29 >.

Category-815: OWASP Top Ten 2010 Category A6 - Security Misconfiguration

Category ID : 815

Summary

Weaknesses in this category are related to the A6 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	B	209	Generation of Error Message Containing Sensitive Information	809	540
HasMember	V	219	Storage of File with Sensitive Data Under Web Root	809	560

Nature	Type	ID	Name	V	Page
HasMember	B	250	Execution with Unnecessary Privileges	809	606
HasMember	B	538	Insertion of Sensitive Information into Externally-Accessible File or Directory	809	1257
HasMember	B	552	Files or Directories Accessible to External Parties	809	1274
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	809	1559

References

[REF-766]OWASP. "Top 10 2010-A6-Security Misconfiguration". < http://www.owasp.org/index.php/Top_10_2010-A6-Security_Misconfiguration >.

Category-816: OWASP Top Ten 2010 Category A7 - Insecure Cryptographic Storage

Category ID : 816

Summary

Weaknesses in this category are related to the A7 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	C	311	Missing Encryption of Sensitive Data	809	764
HasMember	B	312	Cleartext Storage of Sensitive Information	809	771
HasMember	C	326	Inadequate Encryption Strength	809	803
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	809	806
HasMember	V	759	Use of a One-Way Hash without a Salt	809	1593

References

[REF-767]OWASP. "Top 10 2010-A7-Insecure Cryptographic Storage". < http://www.owasp.org/index.php/Top_10_2010-A7-Insecure_Cryptographic_Storage >.

Category-817: OWASP Top Ten 2010 Category A8 - Failure to Restrict URL Access

Category ID : 817

Summary

Weaknesses in this category are related to the A8 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	C	285	Improper Authorization	809	691
HasMember	C	862	Missing Authorization	809	1789
HasMember	C	863	Incorrect Authorization	809	1796

References

[REF-768]OWASP. "Top 10 2010-A8-Failure to Restrict URL Access". < http://www.owasp.org/index.php/Top_10_2010-A8-Failure_to_Restrict_URL_Access >.

Category-818: OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection

Category ID : 818

Summary

Weaknesses in this category are related to the A9 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
MemberOf	C	1346	OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures	1344	2509
HasMember	G	311	Missing Encryption of Sensitive Data	809	764
HasMember	B	319	Cleartext Transmission of Sensitive Information	809	786

References

[REF-769]OWASP. "Top 10 2010-A9-Insufficient Transport Layer Protection". < http://www.owasp.org/index.php/Top_10_2010-A9-Insufficient_Transport_Layer_Protection >.

Category-819: OWASP Top Ten 2010 Category A10 - Unvalidated Redirects and Forwards

Category ID : 819

Summary

Weaknesses in this category are related to the A10 category in the OWASP Top Ten 2010.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	809	Weaknesses in OWASP Top Ten (2010)	809	2584
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	809	1353

References

[REF-770]OWASP. "Top 10 2010-A10-Unvalidated Redirects and Forwards". < http://www.owasp.org/index.php/Top_10_2010-A10-Unvalidated_Redirects_and_Forwards >.

Category-840: Business Logic Errors

Category ID : 840

Summary

Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application. They can be difficult to find automatically, since they typically involve legitimate use of the application's functionality. However, many business logic errors can exhibit patterns that are similar to well-understood implementation and design weaknesses.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576

Nature	Type	ID	Name	V	Page
MemberOf	C	1348	OWASP Top Ten 2021 Category A04:2021 - Insecure Design	1344	2512
HasMember	B	283	Unverified Ownership	699	685
HasMember	B	639	Authorization Bypass Through User-Controlled Key	699	1415
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	699	1418
HasMember	B	708	Incorrect Ownership Assignment	699	1556
HasMember	B	770	Allocation of Resources Without Limits or Throttling	699	1622
HasMember	B	826	Premature Release of Resource During Expected Lifetime	699	1743
HasMember	B	837	Improper Enforcement of a Single, Unique Action	699	1771
HasMember	B	841	Improper Enforcement of Behavioral Workflow	699	1781

Notes

Terminology

The "Business Logic" term is generally used to describe issues that require domain-specific knowledge or "business rules" to determine if they are weaknesses or vulnerabilities, instead of legitimate behavior. Such issues might not be easily detectable via automatic code analysis, because the associated operations do not produce clear errors or undefined behavior at the code level. However, many such "business logic" issues can be understood as instances of other weaknesses such as input validation, access control, numeric computation, order of operations, etc.

Research Gap

The classification of business logic flaws has been under-studied, although exploitation of business flaws frequently happens in real-world systems, and many applied vulnerability researchers investigate them. The greatest focus is in web applications. There is debate within the community about whether these problems represent particularly new concepts, or if they are variations of well-known principles. Many business logic flaws appear to be oriented toward business processes, application flows, and sequences of behaviors, which are not as well-represented in CWE as weaknesses related to input validation, memory management, etc.

References

[REF-795]Jeremiah Grossman. "Business Logic Flaws and Yahoo Games". 2006 December 8. < https://blog.jeremiahgrossman.com/2006/12/business-logic-flaws.html >.2023-04-07.

[REF-796]Jeremiah Grossman. "Seven Business Logic Flaws That Put Your Website At Risk". 2007 October. < https://docplayer.net/10021793-Seven-business-logic-flaws-that-put-your-website-at-risk.html >.2023-04-07.

[REF-797]WhiteHat Security. "Business Logic Flaws". < https://web.archive.org/web/20080720171327/http://www.whitehatsec.com/home/solutions/BL_auction.html >.2023-04-07.

[REF-798]WASC. "Abuse of Functionality". < http://projects.webappsec.org/w/page/13246913/Abuse-of-Functionality >.

[REF-799]Rafal Los and Prajakta Jagdale. "Defying Logic: Theory, Design, and Implementation of Complex Systems for Testing Application Logic". 2011. < https://www.slideshare.net/RafalLos/defying-logic-business-logic-testing-with-automation >.2023-04-07.

[REF-667]Rafal Los. "Real-Life Example of a 'Business Logic Defect' (Screen Shots!)". 2011. < http://h30501.www3.hp.com/t5/Following-the-White-Rabbit-A/Real-Life-Example-of-a-Business-Logic-Defect-Screen-Shots/ba-p/22581 >.

[REF-801]Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel and Giovanni Vigna. "Toward Automated Detection of Logic Vulnerabilities in Web Applications". USENIX Security

Symposium 2010. 2010 August. < https://www.usenix.org/legacy/events/sec10/tech/full_papers/Felmetsger.pdf >.2023-04-07.

[REF-802]Faisal Nabi. "Designing a Framework Method for Secure Business Application Logic Integrity in e-Commerce Systems". International Journal of Network Security, Vol.12, No.1. 2011. < http://ijns.femto.com.tw/contents/ijns-v12-n1/ijns-2011-v12-n1-p29-41.pdf >.

[REF-1102]Chetan Conikee. "Case Files from 20 Years of Business Logic Flaws". 2020 February. < https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18217/2020_USA20_DSO-R02_01_Case%20Files%20from%2020%20Years%20of%20Business%20Logic%20Flaws.pdf >.

Category-845: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 2 - Input Validation and Data Sanitization (IDS)

Category ID : 845

Summary

Weaknesses in this category are related to rules in the Input Validation and Data Sanitization (IDS) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	844	155
HasMember	C	116	Improper Encoding or Escaping of Output	844	287
HasMember	B	134	Use of Externally-Controlled Format String	844	371
HasMember	V	144	Improper Neutralization of Line Delimiters	844	389
HasMember	V	150	Improper Neutralization of Escape, Meta, or Control Sequences	844	400
HasMember	V	180	Incorrect Behavior Order: Validate Before Canonicalize	844	457
HasMember	B	182	Collapse of Data into Unsafe Value	844	462
HasMember	B	289	Authentication Bypass by Alternate Name	844	710
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	844	1004
HasMember	B	625	Permissive Regular Expression	844	1400
HasMember	V	647	Use of Non-Canonical URL Paths for Authorization Decisions	844	1435
HasMember	B	838	Inappropriate Encoding for Output Context	844	1773

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-846: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 3 - Declarations and Initialization (DCL)

Category ID : 846

Summary

Weaknesses in this category are related to rules in the Declarations and Initialization (DCL) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	C	665	Improper Initialization	844	1465

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-847: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 4 - Expressions (EXP)

Category ID : 847

Summary

Weaknesses in this category are related to rules in the Expressions (EXP) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	252	Unchecked Return Value	844	613
HasMember	V	479	Signal Handler Use of a Non-reentrant Function	844	1154
HasMember	V	595	Comparison of Object References Instead of Object Contents	844	1342
HasMember	V	597	Use of Wrong Operator in String Comparison	844	1345

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-848: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 5 - Numeric Types and Operations (NUM)

Category ID : 848

Summary

Weaknesses in this category are related to rules in the Numeric Types and Operations (NUM) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	197	Numeric Truncation Error	844	507
HasMember	B	369	Divide By Zero	844	920
HasMember	B	681	Incorrect Conversion between Numeric Types	844	1504

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-849: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 6 - Object Orientation (OBJ)

Category ID : 849

Summary

Weaknesses in this category are related to rules in the Object Orientation (OBJ) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	374	Passing Mutable Objects to an Untrusted Method	844	927
HasMember	B	375	Returning a Mutable Object to an Untrusted Caller	844	930
HasMember	V	486	Comparison of Classes by Name	844	1172
HasMember	V	491	Public cloneable() Method Without Final ('Object Hijack')	844	1181
HasMember	V	492	Use of Inner Class Containing Sensitive Data	844	1183
HasMember	V	493	Critical Public Variable Without Final Modifier	844	1190
HasMember	V	498	Cloneable Class Containing Sensitive Information	844	1204
HasMember	V	500	Public Static Field Not Marked Final	844	1208
HasMember	V	582	Array Declared Public, Final, and Static	844	1322
HasMember	B	766	Critical Data Element Declared Public	844	1615

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-850: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 7 - Methods (MET)

Category ID : 850

Summary

Weaknesses in this category are related to rules in the Methods (MET) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	487	Reliance on Package-level Scope	844	1175
HasMember	V	568	finalize() Method Without super.finalize()	844	1299
HasMember	C	573	Improper Following of Specification by Caller	844	1307
HasMember	V	581	Object Model Violation: Just One of Equals and Hashcode Defined	844	1321
HasMember	V	583	finalize() Method Declared Public	844	1324
HasMember	B	586	Explicit Call to Finalize()	844	1329
HasMember	V	589	Call to Non-ubiquitous API	844	1333
HasMember	B	617	Reachable Assertion	844	1387

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-851: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 8 - Exceptional Behavior (ERR)

Category ID : 851

Summary

Weaknesses in this category are related to rules in the Exceptional Behavior (ERR) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	209	Generation of Error Message Containing Sensitive Information	844	540
HasMember	V	230	Improper Handling of Missing Values	844	578
HasMember	V	232	Improper Handling of Undefined Values	844	580
HasMember	B	248	Uncaught Exception	844	603
HasMember	V	382	J2EE Bad Practices: Use of System.exit()	844	940
HasMember	B	390	Detection of Error Condition Without Action	844	950
HasMember	B	395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	844	964
HasMember	B	397	Declaration of Throws for Generic Exception	844	968
HasMember	B	460	Improper Cleanup on Thrown Exception	844	1109
HasMember	B	497	Exposure of Sensitive System Information to an Unauthorized Control Sphere	844	1201
HasMember	B	584	Return Inside Finally Block	844	1325
HasMember	V	600	Uncaught Exception in Servlet	844	1352
HasMember	CHAIN	690	Unchecked Return Value to NULL Pointer Dereference	844	1523
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	844	1544
HasMember	C	705	Incorrect Control Flow Scoping	844	1550

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-852: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 9 - Visibility and Atomicity (VNA)

Category ID : 852

Summary

Weaknesses in this category are related to rules in the Visibility and Atomicity (VNA) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	844	895
HasMember	B	366	Race Condition within a Thread	844	910
HasMember	B	413	Improper Resource Locking	844	1010
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	844	1296
HasMember	C	662	Improper Synchronization	844	1457
HasMember	C	667	Improper Locking	844	1472

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-853: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 10 - Locking (LCK)

Category ID : 853

Summary

Weaknesses in this category are related to rules in the Locking (LCK) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	412	Unrestricted Externally Accessible Lock	844	1007
HasMember	B	413	Improper Resource Locking	844	1010
HasMember	B	609	Double-Checked Locking	844	1371
HasMember	C	667	Improper Locking	844	1472
HasMember	B	820	Missing Synchronization	844	1729

Nature	Type	ID	Name	V	Page
HasMember	B	833	Deadlock	844	1762

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-854: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 11 - Thread APIs (THI)

Category ID : 854

Summary

Weaknesses in this category are related to rules in the Thread APIs (THI) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	V	572	Call to Thread run() instead of start()	844	1305
HasMember	C	705	Incorrect Control Flow Scoping	844	1550

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-855: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 12 - Thread Pools (TPS)

Category ID : 855

Summary

Weaknesses in this category are related to rules in the Thread Pools (TPS) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	392	Missing Report of Error Condition	844	958
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	844	993
HasMember	B	410	Insufficient Resource Pool	844	1005

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-856: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 13 - Thread-Safety Miscellaneous (TSM)

Category ID : 856

Summary

Weaknesses in this category are related to rules in the Thread-Safety Miscellaneous (TSM) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-857: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 14 - Input Output (FIO)

Category ID : 857

Summary

Weaknesses in this category are related to rules in the Input Output (FIO) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	V	67	Improper Handling of Windows Device Names	844	127
HasMember	B	135	Incorrect Calculation of Multi-Byte String Length	844	377
HasMember	V	198	Use of Incorrect Byte Ordering	844	510
HasMember	B	276	Incorrect Default Permissions	844	672
HasMember	V	279	Incorrect Execution-Assigned Permissions	844	678
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	844	889
HasMember	C	377	Insecure Temporary File	844	932
HasMember	C	404	Improper Resource Shutdown or Release	844	987
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	844	993
HasMember	B	459	Incomplete Cleanup	844	1106
HasMember	B	532	Insertion of Sensitive Information into Log File	844	1250
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	844	1559
HasMember	B	770	Allocation of Resources Without Limits or Throttling	844	1622

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-858: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 15 - Serialization (SER)

Category ID : 858

Summary

Weaknesses in this category are related to rules in the Serialization (SER) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	250	Execution with Unnecessary Privileges	844	606
HasMember	B	319	Cleartext Transmission of Sensitive Information	844	786
HasMember	C	400	Uncontrolled Resource Consumption	844	971
HasMember	V	499	Serializable Class Containing Sensitive Data	844	1206
HasMember	B	502	Deserialization of Untrusted Data	844	1212
HasMember	V	589	Call to Non-ubiquitous API	844	1333
HasMember	B	770	Allocation of Resources Without Limits or Throttling	844	1622

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-859: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 16 - Platform Security (SEC)

Category ID : 859

Summary

Weaknesses in this category are related to rules in the Platform Security (SEC) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	V	111	Direct Use of Unsafe JNI	844	272
HasMember	B	266	Incorrect Privilege Assignment	844	645
HasMember	B	272	Least Privilege Violation	844	663
HasMember	C	300	Channel Accessible by Non-Endpoint	844	737
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	844	742
HasMember	B	319	Cleartext Transmission of Sensitive Information	844	786
HasMember	B	347	Improper Verification of Cryptographic Signature	844	864
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	844	1125
HasMember	B	494	Download of Code Without Integrity Check	844	1192
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	844	1559
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	844	1723

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-860: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 17 - Runtime Environment (ENV)

Category ID : 860

Summary

Weaknesses in this category are related to rules in the Runtime Environment (ENV) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	844	868
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	844	1559

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-861: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 18 - Miscellaneous (MSC)

Category ID : 861

Summary

Weaknesses in this category are related to rules in the Miscellaneous (MSC) chapter of The CERT Oracle Secure Coding Standard for Java (2011).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	844	Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)	844	2585
HasMember	V	259	Use of Hard-coded Password	844	630
HasMember	C	311	Missing Encryption of Sensitive Data	844	764
HasMember	C	330	Use of Insufficiently Random Values	844	821
HasMember	V	332	Insufficient Entropy in PRNG	844	830
HasMember	V	333	Improper Handling of Insufficient Entropy in TRNG	844	832
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	844	839
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	844	841
HasMember	C	400	Uncontrolled Resource Consumption	844	971

Nature	Type	ID	Name	V	Page
HasMember	V	401	Missing Release of Memory after Effective Lifetime	844	980
HasMember	V	543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	844	1263
HasMember	B	770	Allocation of Resources Without Limits or Throttling	844	1622
HasMember	B	798	Use of Hard-coded Credentials	844	1699

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Category-864: 2011 Top 25 - Insecure Interaction Between Components

Category ID : 864

Summary

Weaknesses in this category are listed in the "Insecure Interaction Between Components" section of the 2011 CWE/SANS Top 25 Most Dangerous Software Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	900	Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors	900	2593
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	900	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	900	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	900	206
HasMember	C	352	Cross-Site Request Forgery (CSRF)	900	875
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	900	1055
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	900	1353
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	900	1750

References

[REF-843]"2011 CWE/SANS Top 25 Most Dangerous Software Errors". 2011 June 7. < https://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.html >.2024-11-17.

Category-865: 2011 Top 25 - Risky Resource Management

Category ID : 865

Summary

Weaknesses in this category are listed in the "Risky Resource Management" section of the 2011 CWE/SANS Top 25 Most Dangerous Software Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	900	Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors	900	2593

Nature	Type	ID	Name	V	Page
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	900	33
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	900	310
HasMember	B	131	Incorrect Calculation of Buffer Size	900	361
HasMember	B	134	Use of Externally-Controlled Format String	900	371
HasMember	B	190	Integer Overflow or Wraparound	900	478
HasMember	B	494	Download of Code Without Integrity Check	900	1192
HasMember	B	676	Use of Potentially Dangerous Function	900	1498

References

[REF-843]"2011 CWE/SANS Top 25 Most Dangerous Software Errors". 2011 June 7. < https://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.html >.2024-11-17.

Category-866: 2011 Top 25 - Porous Defenses

Category ID : 866

Summary

Weaknesses in this category are listed in the "Porous Defenses" section of the 2011 CWE/SANS Top 25 Most Dangerous Software Errors.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	900	Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors	900	2593
HasMember	B	250	Execution with Unnecessary Privileges	900	606
HasMember	B	306	Missing Authentication for Critical Function	900	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	900	754
HasMember	C	311	Missing Encryption of Sensitive Data	900	764
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	900	806
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	900	1559
HasMember	V	759	Use of a One-Way Hash without a Salt	900	1593
HasMember	B	798	Use of Hard-coded Credentials	900	1699
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	900	1723
HasMember	C	862	Missing Authorization	900	1789
HasMember	C	863	Incorrect Authorization	900	1796

References

[REF-843]"2011 CWE/SANS Top 25 Most Dangerous Software Errors". 2011 June 7. < https://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.html >.2024-11-17.

Category-867: 2011 Top 25 - Weaknesses On the Cusp

Category ID : 867

Summary

Weaknesses in this category are not part of the general Top 25, but they were part of the original nominee list from which the Top 25 was drawn.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	900	Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors	900	2593
HasMember	V	129	Improper Validation of Array Index	900	347
HasMember	B	209	Generation of Error Message Containing Sensitive Information	900	540
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	900	551
HasMember	C	330	Use of Insufficiently Random Values	900	821
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	900	895
HasMember	V	456	Missing Initialization of a Variable	900	1096
HasMember	B	476	NULL Pointer Dereference	900	1139
HasMember	B	681	Incorrect Conversion between Numeric Types	900	1504
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	900	1577
HasMember	B	770	Allocation of Resources Without Limits or Throttling	900	1622
HasMember	B	772	Missing Release of Resource after Effective Lifetime	900	1632
HasMember	B	805	Buffer Access with Incorrect Length Value	900	1711
HasMember	B	822	Untrusted Pointer Dereference	900	1732
HasMember	B	825	Expired Pointer Dereference	900	1741
HasMember	B	838	Inappropriate Encoding for Output Context	900	1773
HasMember	B	841	Improper Enforcement of Behavioral Workflow	900	1781

References

[REF-843]"2011 CWE/SANS Top 25 Most Dangerous Software Errors". 2011 June 7. < https://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.html >.2024-11-17.

Category-869: CERT C++ Secure Coding Section 01 - Preprocessor (PRE)

Category ID : 869

Summary

Weaknesses in this category are related to rules in the Preprocessor (PRE) section of the CERT C ++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587

References

[REF-848]The Software Engineering Institute. "01. Preprocessor (PRE)". < https://www.securecoding.cert.org/confluence/display/cplusplus/01.+Preprocessor+%28PRE%29 >.

Category-870: CERT C++ Secure Coding Section 02 - Declarations and Initialization (DCL)

Category ID : 870

Summary

Weaknesses in this category are related to rules in the Declarations and Initialization (DCL) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587

References

[REF-849]CERT. "02. Declarations and Initialization (DCL)". < https://www.securecoding.cert.org/confluence/display/cplusplus/02.+Declarations+and+Initialization+%28DCL%29 >.

Category-871: CERT C++ Secure Coding Section 03 - Expressions (EXP)

Category ID : 871

Summary

Weaknesses in this category are related to rules in the Expressions (EXP) section of the CERT C ++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	B	476	NULL Pointer Dereference	868	1139
HasMember	B	480	Use of Incorrect Operator	868	1157
HasMember	V	768	Incorrect Short Circuit Evaluation	868	1620

References

[REF-850]CERT. "03. Expressions (EXP)". < https://www.securecoding.cert.org/confluence/display/cplusplus/03.+Expressions+%28EXP%29 >.

Category-872: CERT C++ Secure Coding Section 04 - Integers (INT)

Category ID : 872

Summary

Weaknesses in this category are related to rules in the Integers (INT) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	C	20	Improper Input Validation	868	20
HasMember	V	129	Improper Validation of Array Index	868	347
HasMember	B	190	Integer Overflow or Wraparound	868	478
HasMember	V	192	Integer Coercion Error	868	489
HasMember	B	197	Numeric Truncation Error	868	507
HasMember	B	369	Divide By Zero	868	920
HasMember	B	466	Return of Pointer Value Outside of Expected Range	868	1117
HasMember	V	587	Assignment of a Fixed Address to a Pointer	868	1330
HasMember	B	606	Unchecked Input for Loop Condition	868	1366
HasMember	B	676	Use of Potentially Dangerous Function	868	1498
HasMember	B	681	Incorrect Conversion between Numeric Types	868	1504
HasMember	P	682	Incorrect Calculation	868	1507

References

[REF-851]CERT. "04. Integers (INT)". < https://www.securecoding.cert.org/confluence/display/cplusplus/04.+Integers+%28INT%29 >.

Category-873: CERT C++ Secure Coding Section 05 - Floating Point Arithmetic (FLP)

Category ID : 873

Summary

Weaknesses in this category are related to rules in the Floating Point Arithmetic (FLP) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	B	369	Divide By Zero	868	920
HasMember	B	681	Incorrect Conversion between Numeric Types	868	1504
HasMember	P	682	Incorrect Calculation	868	1507
HasMember	V	686	Function Call With Incorrect Argument Type	868	1517

References

[REF-852]CERT. "05. Floating Point Arithmetic (FLP)". < https://www.securecoding.cert.org/confluence/display/cplusplus/05.+Floating+Point+Arithmetic+%28FLP%29 >.

Category-874: CERT C++ Secure Coding Section 06 - Arrays and the STL (ARR)

Category ID : 874

Summary

Weaknesses in this category are related to rules in the Arrays and the STL (ARR) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	868	299
HasMember	V	129	Improper Validation of Array Index	868	347
HasMember	V	467	Use of sizeof() on a Pointer Type	868	1118
HasMember	B	469	Use of Pointer Subtraction to Determine Size	868	1123
HasMember	C	665	Improper Initialization	868	1465
HasMember	B	805	Buffer Access with Incorrect Length Value	868	1711

References

[REF-853]CERT. "06. Arrays and the STL (ARR)". < https://www.securecoding.cert.org/confluence/display/cplusplus/06.+Arrays+and+the+STL+%28ARR%29 >.

Category-875: CERT C++ Secure Coding Section 07 - Characters and Strings (STR)

Category ID : 875

Summary

Weaknesses in this category are related to rules in the Characters and Strings (STR) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	868	155
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	868	198
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	868	299
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	868	310
HasMember	B	170	Improper Null Termination	868	434
HasMember	B	193	Off-by-one Error	868	493
HasMember	B	464	Addition of Data Structure Sentinel	868	1115
HasMember	V	686	Function Call With Incorrect Argument Type	868	1517
HasMember	C	704	Incorrect Type Conversion or Cast	868	1547

References

[REF-854]CERT. "07. Characters and Strings (STR)". < https://www.securecoding.cert.org/confluence/display/cplusplus/07.+Characters+and+Strings+%28STR%29 >.

Category-876: CERT C++ Secure Coding Section 08 - Memory Management (MEM)

Category ID : 876

Summary

Weaknesses in this category are related to rules in the Memory Management (MEM) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	C	20	Improper Input Validation	868	20
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	868	299
HasMember	B	128	Wrap-around Error	868	345
HasMember	B	131	Incorrect Calculation of Buffer Size	868	361
HasMember	B	190	Integer Overflow or Wraparound	868	478
HasMember	B	226	Sensitive Information in Resource Not Removed Before Reuse	868	569
HasMember	V	244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	868	598
HasMember	B	252	Unchecked Return Value	868	613
HasMember	B	391	Unchecked Error Condition	868	955
HasMember	C	404	Improper Resource Shutdown or Release	868	987
HasMember	V	415	Double Free	868	1015
HasMember	V	416	Use After Free	868	1019
HasMember	B	476	NULL Pointer Dereference	868	1139
HasMember	V	528	Exposure of Core Dump File to an Unauthorized Control Sphere	868	1246
HasMember	V	590	Free of Memory not on the Heap	868	1335
HasMember	V	591	Sensitive Data Storage in Improperly Locked Memory	868	1338
HasMember	C	665	Improper Initialization	868	1465
HasMember	V	687	Function Call With Incorrectly Specified Argument Value	868	1518
HasMember	∞	690	Unchecked Return Value to NULL Pointer Dereference	868	1523
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	868	1544
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	868	1577
HasMember	V	762	Mismatched Memory Management Routines	868	1605
HasMember	B	770	Allocation of Resources Without Limits or Throttling	868	1622
HasMember	B	822	Untrusted Pointer Dereference	868	1732

References

[REF-855]CERT. "08. Memory Management (MEM)". < https://www.securecoding.cert.org/confluence/display/cplusplus/08.+Memory+Management+%28MEM%29 >.

Category-877: CERT C++ Secure Coding Section 09 - Input Output (FIO)

Category ID : 877

Summary

Weaknesses in this category are related to rules in the Input Output (FIO) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	868	33
HasMember	V	37	Path Traversal: '/absolute/pathname/here'	868	79
HasMember	V	38	Path Traversal: '\absolute\pathname\here'	868	81
HasMember	V	39	Path Traversal: 'C:dirname'	868	83
HasMember	B	41	Improper Resolution of Path Equivalence	868	87
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	868	112
HasMember	V	62	UNIX Hard Link	868	120
HasMember	V	64	Windows Shortcut Following (.LNK)	868	122
HasMember	V	65	Windows Hard Link	868	124
HasMember	V	67	Improper Handling of Windows Device Names	868	127
HasMember	B	73	External Control of File Name or Path	868	133
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	868	299
HasMember	B	134	Use of Externally-Controlled Format String	868	371
HasMember	B	241	Improper Handling of Unexpected Data Type	868	591
HasMember	B	276	Incorrect Default Permissions	868	672
HasMember	V	279	Incorrect Execution-Assigned Permissions	868	678
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	868	895
HasMember	B	367	Time-of-check Time-of-use (TOCTOU) Race Condition	868	913
HasMember	B	379	Creation of Temporary File in Directory with Insecure Permissions	868	937
HasMember	B	391	Unchecked Error Condition	868	955
HasMember	B	403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	868	985
HasMember	C	404	Improper Resource Shutdown or Release	868	987
HasMember	B	552	Files or Directories Accessible to External Parties	868	1274
HasMember	C	675	Multiple Operations on Resource in Single-Operation Context	868	1496
HasMember	B	676	Use of Potentially Dangerous Function	868	1498
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	868	1559
HasMember	B	770	Allocation of Resources Without Limits or Throttling	868	1622

References

[REF-856]CERT. "09. Input Output (FIO)". < https://www.securecoding.cert.org/confluence/display/cplusplus/09.+Input+Output+%28FIO%29 >.

Category-878: CERT C++ Secure Coding Section 10 - Environment (ENV)

Category ID : 878

Summary

Weaknesses in this category are related to rules in the Environment (ENV) section of the CERT C ++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	868	155
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	868	198
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	868	299
HasMember	B	426	Untrusted Search Path	868	1035
HasMember	V	462	Duplicate Key in Associative List (Alist)	868	1111
HasMember	C	705	Incorrect Control Flow Scoping	868	1550
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	868	1723

References

[REF-857]CERT. "10. Environment (ENV)". < https://www.securecoding.cert.org/confluence/display/cplusplus/10.+Environment+%28ENV%29 >.

Category-879: CERT C++ Secure Coding Section 11 - Signals (SIG)

Category ID : 879

Summary

Weaknesses in this category are related to rules in the Signals (SIG) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	V	479	Signal Handler Use of a Non-reentrant Function	868	1154
HasMember	C	662	Improper Synchronization	868	1457

References

[REF-858]CERT. "11. Signals (SIG)". < https://www.securecoding.cert.org/confluence/display/cplusplus/11.+Signals+%28SIG%29 >.

Category-880: CERT C++ Secure Coding Section 12 - Exceptions and Error Handling (ERR)

Category ID : 880

Summary

Weaknesses in this category are related to rules in the Exceptions and Error Handling (ERR) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	B	209	Generation of Error Message Containing Sensitive Information	868	540
HasMember	B	390	Detection of Error Condition Without Action	868	950
HasMember	B	391	Unchecked Error Condition	868	955
HasMember	B	460	Improper Cleanup on Thrown Exception	868	1109
HasMember	B	497	Exposure of Sensitive System Information to an Unauthorized Control Sphere	868	1201
HasMember	B	544	Missing Standardized Error Handling Mechanism	868	1265
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	868	1544
HasMember	C	705	Incorrect Control Flow Scoping	868	1550
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	868	1577
HasMember	C	755	Improper Handling of Exceptional Conditions	868	1585

References

[REF-861]CERT. "12. Exceptions and Error Handling (ERR)". < https://www.securecoding.cert.org/confluence/display/cplusplus/12.+Exceptions+and+Error+Handling+%28ERR%29 >.

Category-881: CERT C++ Secure Coding Section 13 - Object Oriented Programming (OOP)

Category ID : 881

Summary

Weaknesses in this category are related to rules in the Object Oriented Programming (OOP) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587

References

[REF-862]CERT. "13. Object Oriented Programming (OOP)". < https://www.securecoding.cert.org/confluence/display/cplusplus/13.+Object+Oriented+Programming+%28OOP%29 >.

Category-882: CERT C++ Secure Coding Section 14 - Concurrency (CON)

Category ID : 882

Summary

Weaknesses in this category are related to rules in the Concurrency (CON) section of the CERT C ++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	868	895
HasMember	B	366	Race Condition within a Thread	868	910
HasMember	C	404	Improper Resource Shutdown or Release	868	987
HasMember	B	488	Exposure of Data Element to Wrong Session	868	1176
HasMember	B	772	Missing Release of Resource after Effective Lifetime	868	1632

References

[REF-863]CERT. "14. Concurrency (CON)". < https://www.securecoding.cert.org/confluence/display/cplusplus/14.+Concurrency+%28CON%29 >.

Category-883: CERT C++ Secure Coding Section 49 - Miscellaneous (MSC)

Category ID : 883

Summary

Weaknesses in this category are related to rules in the Miscellaneous (MSC) section of the CERT C++ Secure Coding Standard. Since not all rules map to specific weaknesses, this category may be incomplete.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	868	Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)	868	2587
HasMember	V	14	Compiler Removal of Code to Clear Buffers	868	14
HasMember	C	20	Improper Input Validation	868	20
HasMember	C	116	Improper Encoding or Escaping of Output	868	287
HasMember	V	176	Improper Handling of Unicode Encoding	868	446
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	868	806
HasMember	C	330	Use of Insufficiently Random Values	868	821
HasMember	B	480	Use of Incorrect Operator	868	1157
HasMember	V	482	Comparing instead of Assigning	868	1165
HasMember	B	561	Dead Code	868	1283
HasMember	B	563	Assignment to Variable without Use	868	1289
HasMember	B	570	Expression is Always False	868	1300
HasMember	B	571	Expression is Always True	868	1303
HasMember	P	697	Incorrect Comparison	868	1538
HasMember	C	704	Incorrect Type Conversion or Cast	868	1547

References

[REF-864]CERT. "49. Miscellaneous (MSC)". < https://www.securecoding.cert.org/confluence/display/cplusplus/49.+Miscellaneous+%28MSC%29 >.

Category-885: SFP Primary Cluster: Risky Values

Category ID : 885

Summary

This category identifies Software Fault Patterns (SFPs) within the Risky Values cluster (SFP1).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	998	SFP Secondary Cluster: Glitch in Computation	888	2440

Category-886: SFP Primary Cluster: Unused entities

Category ID : 886

Summary

This category identifies Software Fault Patterns (SFPs) within the Unused entities cluster (SFP2).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	V	482	Comparing instead of Assigning	888	1165
HasMember	B	561	Dead Code	888	1283
HasMember	B	563	Assignment to Variable without Use	888	1289

Category-887: SFP Primary Cluster: API

Category ID : 887

Summary

This category identifies Software Fault Patterns (SFPs) within the API cluster (SFP3).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	1001	SFP Secondary Cluster: Use of an Improper API	888	2441

Category-889: SFP Primary Cluster: Exception Management

Category ID : 889

Summary

This category identifies Software Fault Patterns (SFPs) within the Exception Management cluster (SFP4, SFP5, SFP6).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592

Nature	Type	ID	Name	V	Page
HasMember	C	960	SFP Secondary Cluster: Ambiguous Exception Type	888	2420
HasMember	C	961	SFP Secondary Cluster: Incorrect Exception Behavior	888	2420
HasMember	C	962	SFP Secondary Cluster: Unchecked Status Condition	888	2421

Category-890: SFP Primary Cluster: Memory Access

Category ID : 890

Summary

This category identifies Software Fault Patterns (SFPs) within the Memory Access cluster (SFP7, SFP8).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	970	SFP Secondary Cluster: Faulty Buffer Access	888	2426
HasMember	C	971	SFP Secondary Cluster: Faulty Pointer Use	888	2426
HasMember	C	972	SFP Secondary Cluster: Faulty String Expansion	888	2426
HasMember	C	973	SFP Secondary Cluster: Improper NULL Termination	888	2427
HasMember	C	974	SFP Secondary Cluster: Incorrect Buffer Length Computation	888	2427

Category-891: SFP Primary Cluster: Memory Management

Category ID : 891

Summary

This category identifies Software Fault Patterns (SFPs) within the Memory Management cluster (SFP38).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	969	SFP Secondary Cluster: Faulty Memory Release	888	2425

Category-892: SFP Primary Cluster: Resource Management

Category ID : 892

Summary

This category identifies Software Fault Patterns (SFPs) within the Resource Management cluster (SFP37).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	982	SFP Secondary Cluster: Failure to Release Resource	888	2431

Nature	Type	ID	Name	V	Page
HasMember	C	983	SFP Secondary Cluster: Faulty Resource Use	888	2431
HasMember	C	984	SFP Secondary Cluster: Life Cycle	888	2432
HasMember	C	985	SFP Secondary Cluster: Unrestricted Consumption	888	2432

Category-893: SFP Primary Cluster: Path Resolution

Category ID : 893

Summary

This category identifies Software Fault Patterns (SFPs) within the Path Resolution cluster (SFP16, SFP17, SFP18).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	979	SFP Secondary Cluster: Failed Chroot Jail	888	2429
HasMember	C	980	SFP Secondary Cluster: Link in Resource Name Resolution	888	2430
HasMember	C	981	SFP Secondary Cluster: Path Traversal	888	2430

Category-894: SFP Primary Cluster: Synchronization

Category ID : 894

Summary

This category identifies Software Fault Patterns (SFPs) within the Synchronization cluster (SFP19, SFP20, SFP21, SFP22).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	986	SFP Secondary Cluster: Missing Lock	888	2432
HasMember	C	987	SFP Secondary Cluster: Multiple Locks/Unlocks	888	2433
HasMember	C	988	SFP Secondary Cluster: Race Condition Window	888	2433
HasMember	C	989	SFP Secondary Cluster: Unrestricted Lock	888	2434

Category-895: SFP Primary Cluster: Information Leak

Category ID : 895

Summary

This category identifies Software Fault Patterns (SFPs) within the Information Leak cluster (SFP23).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592

Nature	Type	ID	Name	V	Page
HasMember	C	963	SFP Secondary Cluster: Exposed Data	888	2421
HasMember	C	964	SFP Secondary Cluster: Exposure Temporary File	888	2423
HasMember	C	965	SFP Secondary Cluster: Insecure Session Management	888	2424
HasMember	C	966	SFP Secondary Cluster: Other Exposures	888	2424
HasMember	C	967	SFP Secondary Cluster: State Disclosure	888	2424

Category-896: SFP Primary Cluster: Tainted Input

Category ID : 896

Summary

This category identifies Software Fault Patterns (SFPs) within the Tainted Input cluster (SFP24, SFP25, SFP26, SFP27).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	990	SFP Secondary Cluster: Tainted Input to Command	888	2434
HasMember	C	991	SFP Secondary Cluster: Tainted Input to Environment	888	2437
HasMember	C	992	SFP Secondary Cluster: Faulty Input Transformation	888	2437
HasMember	C	993	SFP Secondary Cluster: Incorrect Input Handling	888	2438
HasMember	C	994	SFP Secondary Cluster: Tainted Input to Variable	888	2438

Category-897: SFP Primary Cluster: Entry Points

Category ID : 897

Summary

This category identifies Software Fault Patterns (SFPs) within the Entry Points cluster (SFP28).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	1002	SFP Secondary Cluster: Unexpected Entry Points	888	2442

Category-898: SFP Primary Cluster: Authentication

Category ID : 898

Summary

This category identifies Software Fault Patterns (SFPs) within the Authentication cluster (SFP29, SFP30, SFP31, SFP32, SFP33, SFP34).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	947	SFP Secondary Cluster: Authentication Bypass	888	2415

Nature	Type	ID	Name	V	Page
HasMember	C	948	SFP Secondary Cluster: Digital Certificate	888	2416
HasMember	C	949	SFP Secondary Cluster: Faulty Endpoint Authentication	888	2416
HasMember	C	950	SFP Secondary Cluster: Hardcoded Sensitive Data	888	2417
HasMember	C	951	SFP Secondary Cluster: Insecure Authentication Policy	888	2417
HasMember	C	952	SFP Secondary Cluster: Missing Authentication	888	2417
HasMember	C	953	SFP Secondary Cluster: Missing Endpoint Authentication	888	2418
HasMember	C	954	SFP Secondary Cluster: Multiple Binds to the Same Port	888	2418
HasMember	C	955	SFP Secondary Cluster: Unrestricted Authentication	888	2418

Category-899: SFP Primary Cluster: Access Control

Category ID : 899

Summary

This category identifies Software Fault Patterns (SFPs) within the Access Control cluster (SFP35).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	944	SFP Secondary Cluster: Access Management	888	2414
HasMember	C	945	SFP Secondary Cluster: Insecure Resource Access	888	2415
HasMember	C	946	SFP Secondary Cluster: Insecure Resource Permissions	888	2415

Category-901: SFP Primary Cluster: Privilege

Category ID : 901

Summary

This category identifies Software Fault Patterns (SFPs) within the Privilege cluster (SFP36).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	V	9	J2EE Misconfiguration: Weak Access Permissions for EJB Methods	888	8
HasMember	B	250	Execution with Unnecessary Privileges	888	606
HasMember	B	266	Incorrect Privilege Assignment	888	645
HasMember	B	267	Privilege Defined With Unsafe Actions	888	648
HasMember	B	268	Privilege Chaining	888	651
HasMember	C	269	Improper Privilege Management	888	653
HasMember	B	270	Privilege Context Switching Error	888	659
HasMember	C	271	Privilege Dropping / Lowering Errors	888	660
HasMember	B	272	Least Privilege Violation	888	663
HasMember	B	274	Improper Handling of Insufficient Privileges	888	670
HasMember	V	520	.NET Misconfiguration: Use of Impersonation	888	1230

Nature	Type	ID	Name	V	Page
HasMember	C	653	Improper Isolation or Compartmentalization	888	1445

Category-902: SFP Primary Cluster: Channel

Category ID : 902

Summary

This category identifies Software Fault Patterns (SFPs) within the Channel cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	956	SFP Secondary Cluster: Channel Attack	888	2418
HasMember	C	957	SFP Secondary Cluster: Protocol Error	888	2419

Category-903: SFP Primary Cluster: Cryptography

Category ID : 903

Summary

This category identifies Software Fault Patterns (SFPs) within the Cryptography cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	958	SFP Secondary Cluster: Broken Cryptography	888	2419
HasMember	C	959	SFP Secondary Cluster: Weak Cryptography	888	2419

Category-904: SFP Primary Cluster: Malware

Category ID : 904

Summary

This category identifies Software Fault Patterns (SFPs) within the Malware cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	V	69	Improper Handling of Windows ::DATA Alternate Data Stream	888	130
HasMember	C	506	Embedded Malicious Code	888	1218
HasMember	B	507	Trojan Horse	888	1220
HasMember	B	508	Non-Replicating Malicious Code	888	1221
HasMember	B	509	Replicating Malicious Code (Virus or Worm)	888	1222
HasMember	B	510	Trapdoor	888	1223
HasMember	B	511	Logic/Time Bomb	888	1225
HasMember	B	512	Spyware	888	1226

Nature	Type	ID	Name	V	Page
HasMember	C	968	SFP Secondary Cluster: Covert Channel	888	2425

Category-905: SFP Primary Cluster: Predictability

Category ID : 905

Summary

This category identifies Software Fault Patterns (SFPs) within the Predictability cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	G	330	Use of Insufficiently Random Values	888	821
HasMember	B	331	Insufficient Entropy	888	828
HasMember	V	332	Insufficient Entropy in PRNG	888	830
HasMember	V	333	Improper Handling of Insufficient Entropy in TRNG	888	832
HasMember	B	334	Small Space of Random Values	888	834
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	888	836
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	888	839
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	888	841
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	888	844
HasMember	V	339	Small Seed Space in PRNG	888	847
HasMember	G	340	Generation of Predictable Numbers or Identifiers	888	849
HasMember	B	341	Predictable from Observable State	888	850
HasMember	B	342	Predictable Exact Value from Previous Values	888	852
HasMember	B	343	Predictable Value Range from Previous Values	888	854
HasMember	B	344	Use of Invariant Value in Dynamically Changing Context	888	856

Category-906: SFP Primary Cluster: UI

Category ID : 906

Summary

This category identifies Software Fault Patterns (SFPs) within the UI cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	995	SFP Secondary Cluster: Feature	888	2439
HasMember	C	996	SFP Secondary Cluster: Security	888	2439
HasMember	C	997	SFP Secondary Cluster: Information Loss	888	2439

Category-907: SFP Primary Cluster: Other

Category ID : 907

Summary

This category identifies Software Fault Patterns (SFPs) within the Other cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	C	975	SFP Secondary Cluster: Architecture	888	2427
HasMember	C	976	SFP Secondary Cluster: Compiler	888	2428
HasMember	C	977	SFP Secondary Cluster: Design	888	2428
HasMember	C	978	SFP Secondary Cluster: Implementation	888	2429

Category-929: OWASP Top Ten 2013 Category A1 - Injection

Category ID : 929

Summary

Weaknesses in this category are related to the A1 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	B	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	928	138
HasMember	B	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	928	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	928	155
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	928	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	928	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	928	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	928	220
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	928	1428
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	928	1444

References

[REF-927]OWASP. "Top 10 2013-A1-Injection". < https://www.owasp.org/index.php/Top_10_2013-A1-Injection >.

Category-930: OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management

Category ID : 930

Summary

Weaknesses in this category are related to the A2 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	B	256	Plaintext Storage of a Password	928	622
HasMember	C	287	Improper Authentication	928	699
HasMember	C	311	Missing Encryption of Sensitive Data	928	764
HasMember	B	384	Session Fixation	928	943
HasMember	C	522	Insufficiently Protected Credentials	928	1234
HasMember	B	523	Unprotected Transport of Credentials	928	1239
HasMember	B	613	Insufficient Session Expiration	928	1380
HasMember	B	620	Unverified Password Change	928	1392
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	928	1418

References

[REF-929]OWASP. "Top 10 2013-A2-Broken Authentication and Session Management". < https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management >.

Category-931: OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS)

Category ID : 931

Summary

Weaknesses in this category are related to the A3 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	928	168

References

[REF-930]OWASP. "Top 10 2013-A3-Cross-Site Scripting (XSS)". < https://www.owasp.org/index.php/Top_10_2013-A3-Cross-Site_Scripting_%28XSS%29 >.

Category-932: OWASP Top Ten 2013 Category A4 - Insecure Direct Object References

Category ID : 932

Summary

Weaknesses in this category are related to the A4 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595

Nature	Type	ID	Name	V	Page
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	928	33
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	928	249
HasMember	B	639	Authorization Bypass Through User-Controlled Key	928	1415
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	928	1553

References

[REF-931]OWASP. "Top 10 2013-A4-Insecure Direct Object References". < https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References >.

Category-933: OWASP Top Ten 2013 Category A5 - Security Misconfiguration

Category ID : 933

Summary

Weaknesses in this category are related to the A5 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	C	2	7PK - Environment	928	2329
HasMember	C	16	Configuration	928	2330
HasMember	B	209	Generation of Error Message Containing Sensitive Information	928	540
HasMember	B	215	Insertion of Sensitive Information Into Debugging Code	928	558
HasMember	V	548	Exposure of Information Through Directory Listing	928	1269

References

[REF-932]OWASP. "Top 10 2013-A5-Security Misconfiguration". < https://www.owasp.org/index.php/Top_10_2013-A5-Security_Misconfiguration >.

Category-934: OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure

Category ID : 934

Summary

Weaknesses in this category are related to the A6 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	C	311	Missing Encryption of Sensitive Data	928	764
HasMember	B	312	Cleartext Storage of Sensitive Information	928	771
HasMember	B	319	Cleartext Transmission of Sensitive Information	928	786
HasMember	C	320	Key Management Errors	928	2340
HasMember	B	325	Missing Cryptographic Step	928	801
HasMember	C	326	Inadequate Encryption Strength	928	803
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	928	806

Nature	Type	ID	Name	V	Page
HasMember	B	328	Use of Weak Hash	928	813

References

[REF-933]OWASP. "Top 10 2013-A6-Sensitive Data Exposure". < https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure >.

Category-935: OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control

Category ID : 935

Summary

Weaknesses in this category are related to the A7 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	C	285	Improper Authorization	928	691

References

[REF-934]OWASP. "Top 10 2013-A7-Missing Function Level Access Control". < https://www.owasp.org/index.php/Top_10_2013-A7-Missing_Function_Level_Access_Control >.

Category-936: OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF)

Category ID : 936

Summary

Weaknesses in this category are related to the A8 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	B	352	Cross-Site Request Forgery (CSRF)	928	875

References

[REF-935]OWASP. "Top 10 2013-A8-Cross-Site Request Forgery (CSRF)". < https://www.owasp.org/index.php/Top_10_2013-A8-Cross-Site_Request_Forgery_%28CSRF%29 >.

Category-937: OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities

Category ID : 937

Summary

Weaknesses in this category are related to the A9 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
MemberOf	C	1352	OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components	1344	2515

Notes

Relationship

This is an unusual category. CWE does not cover the limitations of human processes and procedures that cannot be described in terms of a specific technical weakness as resident in the code, architecture, or configuration of the software. Since "known vulnerabilities" can arise from any kind of weakness, it is not possible to map this OWASP category to other CWE entries, since it would effectively require mapping this category to ALL weaknesses.

References

[REF-936]OWASP. "Top 10 2013-A9-Using Components with Known Vulnerabilities". < https://www.owasp.org/index.php/Top_10_2013-A9-Using_Components_with_Known_Vulnerabilities >.

Category-938: OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards

Category ID : 938

Summary

Weaknesses in this category are related to the A10 category in the OWASP Top Ten 2013.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	928	Weaknesses in OWASP Top Ten (2013)	928	2595
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	928	1353

References

[REF-937]OWASP. "Top 10 2013-A10-Unvalidated Redirects and Forwards". < https://www.owasp.org/index.php/Top_10_2013-A10-Unvalidated_Redirects_and_Forwards >.

Category-944: SFP Secondary Cluster: Access Management

Category ID : 944

Summary

This category identifies Software Fault Patterns (SFPs) within the Access Management cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	899	SFP Primary Cluster: Access Control	888	2407
HasMember	C	282	Improper Ownership Management	888	683
HasMember	B	283	Unverified Ownership	888	685
HasMember	P	284	Improper Access Control	888	687
HasMember	C	286	Incorrect User Management	888	698
HasMember	B	708	Incorrect Ownership Assignment	888	1556

Category-945: SFP Secondary Cluster: Insecure Resource Access

Category ID : 945

Summary

This category identifies Software Fault Patterns (SFPs) within the Insecure Resource Access cluster (SFP35).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	899	SFP Primary Cluster: Access Control	888	2407
HasMember	C	285	Improper Authorization	888	691
HasMember	C	424	Improper Protection of Alternate Path	888	1031
HasMember	B	639	Authorization Bypass Through User-Controlled Key	888	1415
HasMember	V	650	Trusting HTTP Permission Methods on the Server Side	888	1441

Category-946: SFP Secondary Cluster: Insecure Resource Permissions

Category ID : 946

Summary

This category identifies Software Fault Patterns (SFPs) within the Insecure Resource Permissions cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	899	SFP Primary Cluster: Access Control	888	2407
HasMember	B	276	Incorrect Default Permissions	888	672
HasMember	V	277	Insecure Inherited Permissions	888	675
HasMember	V	278	Insecure Preserved Inherited Permissions	888	676
HasMember	V	279	Incorrect Execution-Assigned Permissions	888	678
HasMember	B	281	Improper Preservation of Permissions	888	681
HasMember	V	560	Use of umask() with chmod-style Argument	888	1282
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	888	1559

Category-947: SFP Secondary Cluster: Authentication Bypass

Category ID : 947

Summary

This category identifies Software Fault Patterns (SFPs) within the Authentication Bypass cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	C	287	Improper Authentication	888	699
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	888	707
HasMember	B	289	Authentication Bypass by Alternate Name	888	710
HasMember	B	303	Incorrect Implementation of Authentication Algorithm	888	744

Nature	Type	ID	Name	V	Page
HasMember	B	304	Missing Critical Step in Authentication	888	745
HasMember	B	305	Authentication Bypass by Primary Weakness	888	747
HasMember	B	308	Use of Single-factor Authentication	888	759
HasMember	B	309	Use of Password System for Primary Authentication	888	761
HasMember	B	603	Use of Client-Side Authentication	888	1363

Category-948: SFP Secondary Cluster: Digital Certificate

Category ID : 948

Summary

This category identifies Software Fault Patterns (SFPs) within the Digital Certificate cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	888	726
HasMember	V	297	Improper Validation of Certificate with Host Mismatch	888	729
HasMember	V	298	Improper Validation of Certificate Expiration	888	733
HasMember	B	299	Improper Check for Certificate Revocation	888	734
HasMember	V	593	Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created	888	1339
HasMember	V	599	Missing Validation of OpenSSL Certificate	888	1350

Category-949: SFP Secondary Cluster: Faulty Endpoint Authentication

Category ID : 949

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Endpoint Authentication cluster (SFP29).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	V	293	Using Referer Field for Authentication	888	717
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	888	742
HasMember	C	345	Insufficient Verification of Data Authenticity	888	858
HasMember	C	346	Origin Validation Error	888	860
HasMember	V	350	Reliance on Reverse DNS Resolution for a Security-Critical Action	888	870
HasMember	B	360	Trust of System Event Data	888	894
HasMember	B	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	888	1273
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	888	1292
HasMember	V	647	Use of Non-Canonical URL Paths for Authorization Decisions	888	1435

Category-950: SFP Secondary Cluster: Hardcoded Sensitive Data

Category ID : 950

Summary

This category identifies Software Fault Patterns (SFPs) within the Hardcoded Sensitive Data cluster (SFP33).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	V	258	Empty Password in Configuration File	888	628
HasMember	V	259	Use of Hard-coded Password	888	630
HasMember	V	321	Use of Hard-coded Cryptographic Key	888	792
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	888	1267

Category-951: SFP Secondary Cluster: Insecure Authentication Policy

Category ID : 951

Summary

This category identifies Software Fault Patterns (SFPs) within the Insecure Authentication Policy cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	B	262	Not Using Password Aging	888	640
HasMember	B	263	Password Aging with Long Expiration	888	643
HasMember	B	521	Weak Password Requirements	888	1231
HasMember	V	556	ASP.NET Misconfiguration: Use of Identity Impersonation	888	1280
HasMember	B	613	Insufficient Session Expiration	888	1380
HasMember	B	645	Overly Restrictive Account Lockout Mechanism	888	1432

Category-952: SFP Secondary Cluster: Missing Authentication

Category ID : 952

Summary

This category identifies Software Fault Patterns (SFPs) within the Missing Authentication cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	B	306	Missing Authentication for Critical Function	888	748
HasMember	B	620	Unverified Password Change	888	1392

Category-953: SFP Secondary Cluster: Missing Endpoint Authentication

Category ID : 953

Summary

This category identifies Software Fault Patterns (SFPs) within the Missing Endpoint Authentication cluster (SFP30).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	V	422	Unprotected Windows Messaging Channel ('Shatter')	888	1029
HasMember	B	425	Direct Request ('Forced Browsing')	888	1032

Category-954: SFP Secondary Cluster: Multiple Binds to the Same Port

Category ID : 954

Summary

This category identifies Software Fault Patterns (SFPs) within the Multiple Binds to the Same Port cluster (SFP32).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	V	605	Multiple Binds to the Same Port	888	1364

Category-955: SFP Secondary Cluster: Unrestricted Authentication

Category ID : 955

Summary

This category identifies Software Fault Patterns (SFPs) within the Unrestricted Authentication cluster (SFP34).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	898	SFP Primary Cluster: Authentication	888	2406
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	888	754

Category-956: SFP Secondary Cluster: Channel Attack

Category ID : 956

Summary

This category identifies Software Fault Patterns (SFPs) within the Channel Attack cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	902	SFP Primary Cluster: Channel	888	2408
HasMember	B	290	Authentication Bypass by Spoofing	888	712
HasMember	B	294	Authentication Bypass by Capture-replay	888	719
HasMember	C	300	Channel Accessible by Non-Endpoint	888	737
HasMember	B	301	Reflection Attack in an Authentication Protocol	888	740
HasMember	B	419	Unprotected Primary Channel	888	1024
HasMember	B	420	Unprotected Alternate Channel	888	1025
HasMember	B	421	Race Condition During Access to Alternate Channel	888	1028
HasMember	C	441	Unintended Proxy or Intermediary ('Confused Deputy')	888	1072

Category-957: SFP Secondary Cluster: Protocol Error

Category ID : 957

Summary

This category identifies Software Fault Patterns (SFPs) within the Protocol Error cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	902	SFP Primary Cluster: Channel	888	2408
HasMember	B	353	Missing Support for Integrity Check	888	881
HasMember	P	435	Improper Interaction Between Multiple Correctly-Behaving Entities	888	1063
HasMember	C	436	Interpretation Conflict	888	1065
HasMember	B	437	Incomplete Model of Endpoint Features	888	1067
HasMember	B	757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')	888	1589

Category-958: SFP Secondary Cluster: Broken Cryptography

Category ID : 958

Summary

This category identifies Software Fault Patterns (SFPs) within the Broken Cryptography cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	903	SFP Primary Cluster: Cryptography	888	2408
HasMember	B	325	Missing Cryptographic Step	888	801
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	888	806
HasMember	B	328	Use of Weak Hash	888	813
HasMember	V	759	Use of a One-Way Hash without a Salt	888	1593
HasMember	V	760	Use of a One-Way Hash with a Predictable Salt	888	1598

Category-959: SFP Secondary Cluster: Weak Cryptography

Category ID : 959

Summary

This category identifies Software Fault Patterns (SFPs) within the Weak Cryptography cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	903	SFP Primary Cluster: Cryptography	888	2408
HasMember	B	261	Weak Encoding for Password	888	638
HasMember	B	322	Key Exchange without Entity Authentication	888	795
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	888	797
HasMember	B	324	Use of a Key Past its Expiration Date	888	799
HasMember	C	326	Inadequate Encryption Strength	888	803
HasMember	V	329	Generation of Predictable IV with CBC Mode	888	818
HasMember	B	347	Improper Verification of Cryptographic Signature	888	864
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	888	1418

Category-960: SFP Secondary Cluster: Ambiguous Exception Type

Category ID : 960

Summary

This category identifies Software Fault Patterns (SFPs) within the Ambiguous Exception Type cluster (SFP5).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	889	SFP Primary Cluster: Exception Management	888	2403
HasMember	B	396	Declaration of Catch for Generic Exception	888	966
HasMember	B	397	Declaration of Throws for Generic Exception	888	968

Category-961: SFP Secondary Cluster: Incorrect Exception Behavior

Category ID : 961

Summary

This category identifies Software Fault Patterns (SFPs) within the Incorrect Exception Behavior cluster (SFP6).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	889	SFP Primary Cluster: Exception Management	888	2403
HasMember	B	392	Missing Report of Error Condition	888	958
HasMember	B	393	Return of Wrong Status Code	888	960
HasMember	B	455	Non-exit on Failed Initialization	888	1095
HasMember	B	460	Improper Cleanup on Thrown Exception	888	1109
HasMember	B	544	Missing Standardized Error Handling Mechanism	888	1265
HasMember	B	584	Return Inside Finally Block	888	1325
HasMember	C	636	Not Failing Securely ('Failing Open')	888	1409

Nature	Type	ID	Name	V	Page
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	888	1544

Category-962: SFP Secondary Cluster: Unchecked Status Condition

Category ID : 962

Summary

This category identifies Software Fault Patterns (SFPs) within the Unchecked Status Condition cluster (SFP4).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	889	SFP Primary Cluster: Exception Management	888	2403
HasMember	B	248	Uncaught Exception	888	603
HasMember	B	252	Unchecked Return Value	888	613
HasMember	B	253	Incorrect Check of Function Return Value	888	620
HasMember	B	273	Improper Check for Dropped Privileges	888	667
HasMember	B	280	Improper Handling of Insufficient Permissions or Privileges	888	679
HasMember	B	372	Incomplete Internal State Distinction	888	926
HasMember	B	390	Detection of Error Condition Without Action	888	950
HasMember	B	391	Unchecked Error Condition	888	955
HasMember	B	394	Unexpected Status Code or Return Value	888	962
HasMember	B	395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	888	964
HasMember	B	431	Missing Handler	888	1051
HasMember	B	478	Missing Default Case in Multiple Condition Expression	888	1149
HasMember	B	484	Omitted Break Statement in Switch	888	1169
HasMember	V	600	Uncaught Exception in Servlet	888	1352
HasMember	C	665	Improper Initialization	888	1465
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	888	1577
HasMember	C	755	Improper Handling of Exceptional Conditions	888	1585

Category-963: SFP Secondary Cluster: Exposed Data

Category ID : 963

Summary

This category identifies Software Fault Patterns (SFPs) within the Exposed Data cluster (SFP23).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	895	SFP Primary Cluster: Information Leak	888	2405
HasMember	V	5	J2EE Misconfiguration: Data Transmission Without Encryption	888	1
HasMember	V	7	J2EE Misconfiguration: Missing Custom Error Page	888	4
HasMember	V	8	J2EE Misconfiguration: Entity Bean Declared Remote	888	6
HasMember	V	11	ASP.NET Misconfiguration: Creating Debug Binary	888	9

Nature	Type	ID	Name	V	Page
HasMember	V	12	ASP.NET Misconfiguration: Missing Custom Error Page	888	11
HasMember	V	13	ASP.NET Misconfiguration: Password in Configuration File	888	13
HasMember	V	14	Compiler Removal of Code to Clear Buffers	888	14
HasMember	B	117	Improper Output Neutralization for Logs	888	294
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	888	511
HasMember	B	201	Insertion of Sensitive Information Into Sent Data	888	521
HasMember	B	209	Generation of Error Message Containing Sensitive Information	888	540
HasMember	B	210	Self-generated Error Message Containing Sensitive Information	888	546
HasMember	B	211	Externally-Generated Error Message Containing Sensitive Information	888	548
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	888	551
HasMember	B	213	Exposure of Sensitive Information Due to Incompatible Policies	888	555
HasMember	B	214	Invocation of Process Using Visible Sensitive Information	888	556
HasMember	B	215	Insertion of Sensitive Information Into Debugging Code	888	558
HasMember	V	219	Storage of File with Sensitive Data Under Web Root	888	560
HasMember	V	220	Storage of File With Sensitive Data Under FTP Root	888	562
HasMember	B	226	Sensitive Information in Resource Not Removed Before Reuse	888	569
HasMember	V	244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	888	598
HasMember	B	256	Plaintext Storage of a Password	888	622
HasMember	B	257	Storing Passwords in a Recoverable Format	888	625
HasMember	B	260	Password in Configuration File	888	636
HasMember	C	311	Missing Encryption of Sensitive Data	888	764
HasMember	B	312	Cleartext Storage of Sensitive Information	888	771
HasMember	V	313	Cleartext Storage in a File or on Disk	888	777
HasMember	V	314	Cleartext Storage in the Registry	888	779
HasMember	V	315	Cleartext Storage of Sensitive Information in a Cookie	888	781
HasMember	V	316	Cleartext Storage of Sensitive Information in Memory	888	782
HasMember	V	317	Cleartext Storage of Sensitive Information in GUI	888	784
HasMember	V	318	Cleartext Storage of Sensitive Information in Executable	888	785
HasMember	B	319	Cleartext Transmission of Sensitive Information	888	786
HasMember	B	374	Passing Mutable Objects to an Untrusted Method	888	927
HasMember	B	375	Returning a Mutable Object to an Untrusted Caller	888	930
HasMember	C	402	Transmission of Private Resources into a New Sphere ('Resource Leak')	888	984
HasMember	B	403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	888	985
HasMember	V	433	Unparsed Raw Web Content Delivery	888	1053
HasMember	V	495	Private Data Structure Returned From A Public Method	888	1197
HasMember	B	497	Exposure of Sensitive System Information to an Unauthorized Control Sphere	888	1201
HasMember	V	498	Cloneable Class Containing Sensitive Information	888	1204
HasMember	V	499	Serializable Class Containing Sensitive Data	888	1206

Nature	Type	ID	Name	V	Page
HasMember	B	501	Trust Boundary Violation	888	1210
HasMember	C	522	Insufficiently Protected Credentials	888	1234
HasMember	B	523	Unprotected Transport of Credentials	888	1239
HasMember	V	526	Cleartext Storage of Sensitive Information in an Environment Variable	888	1243
HasMember	V	527	Exposure of Version-Control Repository to an Unauthorized Control Sphere	888	1245
HasMember	V	528	Exposure of Core Dump File to an Unauthorized Control Sphere	888	1246
HasMember	V	529	Exposure of Access Control List Files to an Unauthorized Control Sphere	888	1247
HasMember	V	530	Exposure of Backup File to an Unauthorized Control Sphere	888	1248
HasMember	B	532	Insertion of Sensitive Information into Log File	888	1250
HasMember	V	535	Exposure of Information Through Shell Error Message	888	1253
HasMember	V	536	Servlet Runtime Error Message Containing Sensitive Information	888	1254
HasMember	V	537	Java Runtime Error Message Containing Sensitive Information	888	1255
HasMember	B	538	Insertion of Sensitive Information into Externally-Accessible File or Directory	888	1257
HasMember	V	539	Use of Persistent Cookies Containing Sensitive Information	888	1259
HasMember	B	540	Inclusion of Sensitive Information in Source Code	888	1260
HasMember	V	541	Inclusion of Sensitive Information in an Include File	888	1262
HasMember	V	546	Suspicious Comment	888	1266
HasMember	V	548	Exposure of Information Through Directory Listing	888	1269
HasMember	V	550	Server-generated Error Message Containing Sensitive Information	888	1272
HasMember	B	552	Files or Directories Accessible to External Parties	888	1274
HasMember	V	555	J2EE Misconfiguration: Plaintext Password in Configuration File	888	1279
HasMember	V	591	Sensitive Data Storage in Improperly Locked Memory	888	1338
HasMember	V	598	Use of GET Request Method With Sensitive Query Strings	888	1349
HasMember	V	607	Public Static Final Field References Mutable Object	888	1368
HasMember	B	612	Improper Authorization of Index Containing Sensitive Information	888	1379
HasMember	V	615	Inclusion of Sensitive Information in Source Code Comments	888	1383
HasMember	C	642	External Control of Critical State Data	888	1422
HasMember	C	668	Exposure of Resource to Wrong Sphere	888	1478
HasMember	C	669	Incorrect Resource Transfer Between Spheres	888	1480
HasMember	B	756	Missing Custom Error Page	888	1588
HasMember	B	767	Access to Critical Private Variable via Public Method	888	1619

Category-964: SFP Secondary Cluster: Exposure Temporary File

Category ID : 964

Summary

This category identifies Software Fault Patterns (SFPs) within the Exposure Temporary File cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	895	SFP Primary Cluster: Information Leak	888	2405
HasMember	C	377	Insecure Temporary File	888	932
HasMember	B	378	Creation of Temporary File With Insecure Permissions	888	935
HasMember	B	379	Creation of Temporary File in Directory with Insecure Permissions	888	937

Category-965: SFP Secondary Cluster: Insecure Session Management

Category ID : 965

Summary

This category identifies Software Fault Patterns (SFPs) within the Insecure Session Management cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	895	SFP Primary Cluster: Information Leak	888	2405
HasMember	V	6	J2EE Misconfiguration: Insufficient Session-ID Length	888	2
HasMember	B	488	Exposure of Data Element to Wrong Session	888	1176
HasMember	B	524	Use of Cache Containing Sensitive Information	888	1240

Category-966: SFP Secondary Cluster: Other Exposures

Category ID : 966

Summary

This category identifies Software Fault Patterns (SFPs) within the Other Exposures cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	895	SFP Primary Cluster: Information Leak	888	2405
HasMember	V	453	Insecure Default Variable Initialization	888	1091
HasMember	B	487	Reliance on Package-level Scope	888	1175
HasMember	V	492	Use of Inner Class Containing Sensitive Data	888	1183
HasMember	V	525	Use of Web Browser Cache Containing Sensitive Information	888	1242
HasMember	V	614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	888	1382
HasMember	V	651	Exposure of WSDL File Containing Sensitive Information	888	1442

Category-967: SFP Secondary Cluster: State Disclosure

Category ID : 967

Summary

This category identifies Software Fault Patterns (SFPs) within the State Disclosure cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	895	SFP Primary Cluster: Information Leak	888	2405
HasMember	B	202	Exposure of Sensitive Information Through Data Queries	888	523
HasMember	B	203	Observable Discrepancy	888	525
HasMember	B	204	Observable Response Discrepancy	888	530
HasMember	B	205	Observable Behavioral Discrepancy	888	533
HasMember	V	206	Observable Internal Behavioral Discrepancy	888	534
HasMember	V	207	Observable Behavioral Discrepancy With Equivalent Products	888	535
HasMember	B	208	Observable Timing Discrepancy	888	537

Category-968: SFP Secondary Cluster: Covert Channel

Category ID : 968

Summary

This category identifies Software Fault Patterns (SFPs) within the Covert Channel cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	904	SFP Primary Cluster: Malware	888	2408
HasMember	B	385	Covert Timing Channel	888	947
HasMember	C	514	Covert Channel	888	1227
HasMember	B	515	Covert Storage Channel	888	1229

Category-969: SFP Secondary Cluster: Faulty Memory Release

Category ID : 969

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Memory Release cluster (SFP12).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	891	SFP Primary Cluster: Memory Management	888	2404
HasMember	V	415	Double Free	888	1015
HasMember	V	590	Free of Memory not on the Heap	888	1335
HasMember	V	761	Free of Pointer not at Start of Buffer	888	1601
HasMember	B	763	Release of Invalid Pointer or Reference	888	1608

Category-970: SFP Secondary Cluster: Faulty Buffer Access

Category ID : 970

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Buffer Access cluster (SFP8).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	890	SFP Primary Cluster: Memory Access	888	2404
HasMember	C	118	Incorrect Access of Indexable Resource ('Range Error')	888	298
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	888	299
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	888	310
HasMember	V	121	Stack-based Buffer Overflow	888	320
HasMember	V	122	Heap-based Buffer Overflow	888	324
HasMember	B	123	Write-what-where Condition	888	329
HasMember	B	124	Buffer Underwrite ('Buffer Underflow')	888	332
HasMember	B	125	Out-of-bounds Read	888	336
HasMember	V	126	Buffer Over-read	888	340
HasMember	V	127	Buffer Under-read	888	343
HasMember	V	129	Improper Validation of Array Index	888	347

Category-971: SFP Secondary Cluster: Faulty Pointer Use

Category ID : 971

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Pointer Use cluster (SFP7).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	890	SFP Primary Cluster: Memory Access	888	2404
HasMember	B	469	Use of Pointer Subtraction to Determine Size	888	1123
HasMember	B	476	NULL Pointer Dereference	888	1139
HasMember	V	588	Attempt to Access Child of a Non-structure Pointer	888	1332

Category-972: SFP Secondary Cluster: Faulty String Expansion

Category ID : 972

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty String Expansion cluster (SFP9).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	890	SFP Primary Cluster: Memory Access	888	2404
HasMember	V	785	Use of Path Manipulation Function without Maximum-sized Buffer	888	1664

Category-973: SFP Secondary Cluster: Improper NULL Termination

Category ID : 973

Summary

This category identifies Software Fault Patterns (SFPs) within the Improper NULL Termination cluster (SFP11).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	890	SFP Primary Cluster: Memory Access	888	2404
HasMember	B	170	Improper Null Termination	888	434

Category-974: SFP Secondary Cluster: Incorrect Buffer Length Computation

Category ID : 974

Summary

This category identifies Software Fault Patterns (SFPs) within the Incorrect Buffer Length Computation cluster (SFP10).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	890	SFP Primary Cluster: Memory Access	888	2404
HasMember	B	131	Incorrect Calculation of Buffer Size	888	361
HasMember	B	135	Incorrect Calculation of Multi-Byte String Length	888	377
HasMember	C	251	Often Misused: String Management	888	2335
HasMember	V	467	Use of sizeof() on a Pointer Type	888	1118

Category-975: SFP Secondary Cluster: Architecture

Category ID : 975

Summary

This category identifies Software Fault Patterns (SFPs) within the Architecture cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	907	SFP Primary Cluster: Other	888	2409
HasMember	B	348	Use of Less Trusted Source	888	866
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	888	889
HasMember	G	602	Client-Side Enforcement of Server-Side Security	888	1359

Nature	Type	ID	Name	V	Page
HasMember	C	637	Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism')	888	1411
HasMember	B	649	Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking	888	1439
HasMember	B	654	Reliance on a Single Factor in a Security Decision	888	1448
HasMember	C	656	Reliance on Security Through Obscurity	888	1452
HasMember	C	657	Violation of Secure Design Principles	888	1454
HasMember	C	671	Lack of Administrator Control over Security	888	1487
HasMember	P	693	Protection Mechanism Failure	888	1529
HasMember	B	749	Exposed Dangerous Method or Function	888	1572

Category-976: SFP Secondary Cluster: Compiler

Category ID : 976

Summary

This category identifies Software Fault Patterns (SFPs) within the Compiler cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	907	SFP Primary Cluster: Other	888	2409
HasMember	B	733	Compiler Optimization Removal or Modification of Security-critical Code	888	1570

Category-977: SFP Secondary Cluster: Design

Category ID : 977

Summary

This category identifies Software Fault Patterns (SFPs) within the Design cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	907	SFP Primary Cluster: Other	888	2409
HasMember	B	115	Misinterpretation of Input	888	286
HasMember	V	187	Partial String Comparison	888	474
HasMember	B	188	Reliance on Data/Memory Layout	888	476
HasMember	B	193	Off-by-one Error	888	493
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	888	868
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	888	993
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	888	997
HasMember	C	407	Inefficient Algorithmic Complexity	888	999
HasMember	B	408	Incorrect Behavior Order: Early Amplification	888	1002
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	888	1004
HasMember	B	410	Insufficient Resource Pool	888	1005

Nature	Type	ID	Name	V	Page
HasMember	B	430	Deployment of Wrong Handler	888	1049
HasMember	V	462	Duplicate Key in Associative List (Alist)	888	1111
HasMember	B	463	Deletion of Data Structure Sentinel	888	1113
HasMember	B	464	Addition of Data Structure Sentinel	888	1115
HasMember	B	483	Incorrect Block Delimitation	888	1167
HasMember	V	581	Object Model Violation: Just One of Equals and Hashcode Defined	888	1321
HasMember	V	595	Comparison of Object References Instead of Object Contents	888	1342
HasMember	V	618	Exposed Unsafe ActiveX Method	888	1389
HasMember	B	648	Incorrect Use of Privileged APIs	888	1437
HasMember	C	670	Always-Incorrect Control Flow Implementation	888	1484
HasMember	P	682	Incorrect Calculation	888	1507
HasMember	P	691	Insufficient Control Flow Management	888	1525
HasMember	C	696	Incorrect Behavior Order	888	1535
HasMember	P	697	Incorrect Comparison	888	1538
HasMember	B	698	Execution After Redirect (EAR)	888	1542
HasMember	C	705	Incorrect Control Flow Scoping	888	1550

Category-978: SFP Secondary Cluster: Implementation

Category ID : 978

Summary

This category identifies Software Fault Patterns (SFPs) within the Implementation cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	907	SFP Primary Cluster: Other	888	2409
HasMember	B	358	Improperly Implemented Security Check for Standard	888	888
HasMember	C	398	7PK - Code Quality	888	2344
HasMember	V	623	Unsafe ActiveX Control Marked Safe For Scripting	888	1397
HasMember	P	710	Improper Adherence to Coding Standards	888	1558

Category-979: SFP Secondary Cluster: Failed Chroot Jail

Category ID : 979

Summary

This category identifies Software Fault Patterns (SFPs) within the Failed Chroot Jail cluster (SFP17).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	893	SFP Primary Cluster: Path Resolution	888	2405
HasMember	V	243	Creation of chroot Jail Without Changing Working Directory	888	596

Category-980: SFP Secondary Cluster: Link in Resource Name Resolution

Category ID : 980

Summary

This category identifies Software Fault Patterns (SFPs) within the Link in Resource Name Resolution cluster (SFP18).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	893	SFP Primary Cluster: Path Resolution	888	2405
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	888	112
HasMember	V	62	UNIX Hard Link	888	120
HasMember	V	64	Windows Shortcut Following (.LNK)	888	122
HasMember	V	65	Windows Hard Link	888	124
HasMember	B	386	Symbolic Name not Mapping to Correct Object	888	949
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	888	1373

Category-981: SFP Secondary Cluster: Path Traversal

Category ID : 981

Summary

This category identifies Software Fault Patterns (SFPs) within the Path Traversal cluster (SFP16).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	893	SFP Primary Cluster: Path Resolution	888	2405
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	888	33
HasMember	B	23	Relative Path Traversal	888	46
HasMember	V	24	Path Traversal: '../filedir'	888	53
HasMember	V	25	Path Traversal: '/../filedir'	888	55
HasMember	V	26	Path Traversal: '/dir/../filename'	888	57
HasMember	V	27	Path Traversal: 'dir/../../filename'	888	58
HasMember	V	28	Path Traversal: '..\filedir'	888	60
HasMember	V	29	Path Traversal: '\..\filename'	888	62
HasMember	V	30	Path Traversal: '\dir\..\filename'	888	64
HasMember	V	31	Path Traversal: 'dir\..\..\filename'	888	65
HasMember	V	32	Path Traversal: '...' (Triple Dot)	888	67
HasMember	V	33	Path Traversal: '....' (Multiple Dot)	888	69
HasMember	V	34	Path Traversal: '....//'	888	71
HasMember	V	35	Path Traversal: '.../...//'	888	73
HasMember	B	36	Absolute Path Traversal	888	75
HasMember	V	37	Path Traversal: '/absolute/pathname/here'	888	79
HasMember	V	38	Path Traversal: '\absolute\pathname\here'	888	81
HasMember	V	39	Path Traversal: 'C:dirname'	888	83
HasMember	V	40	Path Traversal: '\\UNC\share\name\' (Windows UNC Share)	888	86

Nature	Type	ID	Name	V	Page
HasMember	B	41	Improper Resolution of Path Equivalence	888	87
HasMember	V	42	Path Equivalence: 'filename.' (Trailing Dot)	888	93
HasMember	V	43	Path Equivalence: 'filename....' (Multiple Trailing Dot)	888	94
HasMember	V	44	Path Equivalence: 'file.name' (Internal Dot)	888	95
HasMember	V	45	Path Equivalence: 'file...name' (Multiple Internal Dot)	888	96
HasMember	V	46	Path Equivalence: 'filename ' (Trailing Space)	888	97
HasMember	V	47	Path Equivalence: ' filename' (Leading Space)	888	98
HasMember	V	48	Path Equivalence: 'file name' (Internal Whitespace)	888	99
HasMember	V	49	Path Equivalence: 'filename/' (Trailing Slash)	888	100
HasMember	V	50	Path Equivalence: '//multiple/leading/slash'	888	101
HasMember	V	51	Path Equivalence: '/multiple//internal/slash'	888	103
HasMember	V	52	Path Equivalence: '/multiple/trailing/slash//'	888	104
HasMember	V	53	Path Equivalence: '\multiple\\internal\backslash'	888	105
HasMember	V	54	Path Equivalence: 'filedir\' (Trailing Backslash)	888	106
HasMember	V	55	Path Equivalence: '/./' (Single Dot Directory)	888	107
HasMember	V	56	Path Equivalence: 'filedir*' (Wildcard)	888	108
HasMember	V	57	Path Equivalence: 'fakedir/../realdir/filename'	888	109
HasMember	V	58	Path Equivalence: Windows 8.3 Filename	888	111
HasMember	B	66	Improper Handling of File Names that Identify Virtual Resources	888	125
HasMember	V	67	Improper Handling of Windows Device Names	888	127
HasMember	V	72	Improper Handling of Apple HFS+ Alternate Data Stream Path	888	131
HasMember	B	73	External Control of File Name or Path	888	133
HasMember	B	428	Unquoted Search Path or Element	888	1047
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	888	1553

Category-982: SFP Secondary Cluster: Failure to Release Resource

Category ID : 982

Summary

This category identifies Software Fault Patterns (SFPs) within the Failure to Release Resource cluster (SFP14).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	892	SFP Primary Cluster: Resource Management	888	2404
HasMember	C	404	Improper Resource Shutdown or Release	888	987
HasMember	B	459	Incomplete Cleanup	888	1106
HasMember	B	771	Missing Reference to Active Allocated Resource	888	1631
HasMember	B	772	Missing Release of Resource after Effective Lifetime	888	1632
HasMember	V	773	Missing Reference to Active File Descriptor or Handle	888	1638
HasMember	V	775	Missing Release of File Descriptor or Handle after Effective Lifetime	888	1640

Category-983: SFP Secondary Cluster: Faulty Resource Use

Category ID : 983

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Resource Use cluster (SFP15).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	892	SFP Primary Cluster: Resource Management	888	2404
HasMember	V	416	Use After Free	888	1019
HasMember	C	672	Operation on a Resource after Expiration or Release	888	1488

Category-984: SFP Secondary Cluster: Life Cycle

Category ID : 984

Summary

This category identifies Software Fault Patterns (SFPs) within the Life Cycle cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	892	SFP Primary Cluster: Resource Management	888	2404
HasMember	P	664	Improper Control of a Resource Through its Lifetime	888	1463
HasMember	C	666	Operation on Resource in Wrong Phase of Lifetime	888	1471
HasMember	C	675	Multiple Operations on Resource in Single-Operation Context	888	1496
HasMember	B	694	Use of Multiple Resources with Duplicate Identifier	888	1531

Category-985: SFP Secondary Cluster: Unrestricted Consumption

Category ID : 985

Summary

This category identifies Software Fault Patterns (SFPs) within the Unrestricted Consumption cluster (SFP13).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	892	SFP Primary Cluster: Resource Management	888	2404
HasMember	C	400	Uncontrolled Resource Consumption	888	971
HasMember	C	674	Uncontrolled Recursion	888	1493
HasMember	B	770	Allocation of Resources Without Limits or Throttling	888	1622
HasMember	V	774	Allocation of File Descriptors or Handles Without Limits or Throttling	888	1639

Category-986: SFP Secondary Cluster: Missing Lock

Category ID : 986

Summary

This category identifies Software Fault Patterns (SFPs) within the Missing Lock cluster (SFP19).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	894	SFP Primary Cluster: Synchronization	888	2405
HasMember	B	364	Signal Handler Race Condition	888	905
HasMember	B	366	Race Condition within a Thread	888	910
HasMember	B	368	Context Switching Race Condition	888	918
HasMember	B	413	Improper Resource Locking	888	1010
HasMember	B	414	Missing Lock Check	888	1014
HasMember	V	543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	888	1263
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	888	1296
HasMember	B	609	Double-Checked Locking	888	1371
HasMember	C	662	Improper Synchronization	888	1457
HasMember	B	663	Use of a Non-reentrant Function in a Concurrent Context	888	1461
HasMember	C	667	Improper Locking	888	1472

Category-987: SFP Secondary Cluster: Multiple Locks/Unlocks

Category ID : 987

Summary

This category identifies Software Fault Patterns (SFPs) within the Multiple Locks/Unlocks cluster (SFP21).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	894	SFP Primary Cluster: Synchronization	888	2405
HasMember	V	585	Empty Synchronized Block	888	1327
HasMember	B	764	Multiple Locks of a Critical Resource	888	1613
HasMember	B	765	Multiple Unlocks of a Critical Resource	888	1614

Category-988: SFP Secondary Cluster: Race Condition Window

Category ID : 988

Summary

This category identifies Software Fault Patterns (SFPs) within the Race Condition Window cluster (SFP20).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	894	SFP Primary Cluster: Synchronization	888	2405

Nature	Type	ID	Name	V	Page
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	888	895
HasMember	B	363	Race Condition Enabling Link Following	888	904
HasMember	B	367	Time-of-check Time-of-use (TOCTOU) Race Condition	888	913
HasMember	V	370	Missing Check for Certificate Revocation after Initial Check	888	924
HasMember	C	638	Not Using Complete Mediation	888	1413

Category-989: SFP Secondary Cluster: Unrestricted Lock

Category ID : 989

Summary

This category identifies Software Fault Patterns (SFPs) within the Unrestricted Lock cluster (SFP22).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	894	SFP Primary Cluster: Synchronization	888	2405
HasMember	B	412	Unrestricted Externally Accessible Lock	888	1007

Category-990: SFP Secondary Cluster: Tainted Input to Command

Category ID : 990

Summary

This category identifies Software Fault Patterns (SFPs) within the Tainted Input to Command cluster (SFP24).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	896	SFP Primary Cluster: Tainted Input	888	2406
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	888	138
HasMember	C	75	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)	888	145
HasMember	B	76	Improper Neutralization of Equivalent Special Elements	888	146
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	888	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	888	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	888	168
HasMember	V	80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	888	182
HasMember	V	81	Improper Neutralization of Script in an Error Message Web Page	888	184
HasMember	V	82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	888	186

Nature	Type	ID	Name	V	Page
HasMember	V	83	Improper Neutralization of Script in Attributes in a Web Page	888	188
HasMember	V	84	Improper Neutralization of Encoded URI Schemes in a Web Page	888	190
HasMember	V	85	Doubled Character XSS Manipulations	888	192
HasMember	V	86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	888	194
HasMember	V	87	Improper Neutralization of Alternate XSS Syntax	888	196
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	888	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	888	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	888	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	888	220
HasMember	B	93	Improper Neutralization of CRLF Sequences ('CRLF Injection')	888	222
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	888	232
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	888	238
HasMember	V	97	Improper Neutralization of Server-Side Includes (SSI) Within a Web Page	888	241
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	888	249
HasMember	V	102	Struts: Duplicate Validation Forms	888	252
HasMember	V	103	Struts: Incomplete validate() Method Definition	888	254
HasMember	V	104	Struts: Form Bean Does Not Extend Validation Class	888	257
HasMember	V	105	Struts: Form Field Without Validator	888	259
HasMember	V	106	Struts: Plug-in Framework not in Use	888	262
HasMember	V	107	Struts: Unused Validation Form	888	265
HasMember	V	108	Struts: Unvalidated Action Form	888	267
HasMember	V	109	Struts: Validator Turned Off	888	269
HasMember	V	110	Struts: Validator Without Form Field	888	270
HasMember	B	112	Missing XML Validation	888	275
HasMember	V	113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')	888	277
HasMember	B	130	Improper Handling of Length Parameter Inconsistency	888	357
HasMember	B	134	Use of Externally-Controlled Format String	888	371
HasMember	C	138	Improper Neutralization of Special Elements	888	379
HasMember	B	140	Improper Neutralization of Delimiters	888	382
HasMember	V	141	Improper Neutralization of Parameter/Argument Delimiters	888	384
HasMember	V	142	Improper Neutralization of Value Delimiters	888	386
HasMember	V	143	Improper Neutralization of Record Delimiters	888	387
HasMember	V	144	Improper Neutralization of Line Delimiters	888	389
HasMember	V	145	Improper Neutralization of Section Delimiters	888	391
HasMember	V	146	Improper Neutralization of Expression/Command Delimiters	888	393
HasMember	V	147	Improper Neutralization of Input Terminators	888	395
HasMember	V	148	Improper Neutralization of Input Leaders	888	397

Nature	Type	ID	Name	V	Page
HasMember	V	149	Improper Neutralization of Quoting Syntax	888	398
HasMember	V	150	Improper Neutralization of Escape, Meta, or Control Sequences	888	400
HasMember	V	151	Improper Neutralization of Comment Delimiters	888	402
HasMember	V	152	Improper Neutralization of Macro Symbols	888	404
HasMember	V	153	Improper Neutralization of Substitution Characters	888	406
HasMember	V	154	Improper Neutralization of Variable Name Delimiters	888	407
HasMember	V	155	Improper Neutralization of Wildcards or Matching Symbols	888	409
HasMember	V	156	Improper Neutralization of Whitespace	888	411
HasMember	V	157	Failure to Sanitize Paired Delimiters	888	413
HasMember	V	158	Improper Neutralization of Null Byte or NUL Character	888	415
HasMember	C	159	Improper Handling of Invalid Use of Special Elements	888	417
HasMember	V	160	Improper Neutralization of Leading Special Elements	888	419
HasMember	V	161	Improper Neutralization of Multiple Leading Special Elements	888	421
HasMember	V	162	Improper Neutralization of Trailing Special Elements	888	423
HasMember	V	163	Improper Neutralization of Multiple Trailing Special Elements	888	425
HasMember	V	164	Improper Neutralization of Internal Special Elements	888	426
HasMember	V	165	Improper Neutralization of Multiple Internal Special Elements	888	428
HasMember	B	183	Permissive List of Allowed Inputs	888	464
HasMember	B	184	Incomplete List of Disallowed Inputs	888	466
HasMember	C	185	Incorrect Regular Expression	888	469
HasMember	B	186	Overly Restrictive Regular Expression	888	472
HasMember	B	444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	888	1075
HasMember	V	553	Command Shell in Externally Accessible Directory	888	1277
HasMember	V	554	ASP.NET Misconfiguration: Not Using Input Validation Framework	888	1278
HasMember	V	564	SQL Injection: Hibernate	888	1290
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	888	1353
HasMember	B	611	Improper Restriction of XML External Entity Reference	888	1376
HasMember	B	619	Dangling Database Cursor ('Cursor Injection')	888	1391
HasMember	V	621	Variable Extraction Error	888	1394
HasMember	B	624	Executable Regular Expression Error	888	1399
HasMember	B	625	Permissive Regular Expression	888	1400
HasMember	V	626	Null Byte Interaction Error (Poison Null Byte)	888	1403
HasMember	V	627	Dynamic Variable Evaluation	888	1405
HasMember	B	641	Improper Restriction of Names for Files and Other Resources	888	1421
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	888	1428
HasMember	V	644	Improper Neutralization of HTTP Headers for Scripting Syntax	888	1430
HasMember	V	646	Reliance on File Name or Extension of Externally-Supplied File	888	1434
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	888	1444

Nature	Type	ID	Name	V	Page
HasMember	V	687	Function Call With Incorrectly Specified Argument Value	888	1518
HasMember	P	707	Improper Neutralization	888	1554

Category-991: SFP Secondary Cluster: Tainted Input to Environment

Category ID : 991

Summary

This category identifies Software Fault Patterns (SFPs) within the Tainted Input to Environment cluster (SFP27).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	896	SFP Primary Cluster: Tainted Input	888	2406
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	888	225
HasMember	C	114	Process Control	888	283
HasMember	B	427	Uncontrolled Search Path Element	888	1040
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	888	1125
HasMember	B	471	Modification of Assumed-Immutable Data (MAID)	888	1129
HasMember	B	472	External Control of Assumed-Immutable Web Parameter	888	1131
HasMember	V	473	PHP External Variable Modification	888	1134
HasMember	B	494	Download of Code Without Integrity Check	888	1192
HasMember	V	622	Improper Validation of Function Hook Arguments	888	1396
HasMember	C	673	External Influence of Sphere Definition	888	1492

Category-992: SFP Secondary Cluster: Faulty Input Transformation

Category ID : 992

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Input Transformation cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	896	SFP Primary Cluster: Tainted Input	888	2406
HasMember	C	116	Improper Encoding or Escaping of Output	888	287
HasMember	B	166	Improper Handling of Missing Special Element	888	429
HasMember	B	167	Improper Handling of Additional Special Element	888	431
HasMember	B	168	Improper Handling of Inconsistent Special Elements	888	433
HasMember	C	172	Encoding Error	888	439
HasMember	V	173	Improper Handling of Alternate Encoding	888	441
HasMember	V	174	Double Decoding of the Same Data	888	443
HasMember	V	175	Improper Handling of Mixed Encoding	888	445
HasMember	V	176	Improper Handling of Unicode Encoding	888	446

Nature	Type	ID	Name	V	Page
HasMember	V	177	Improper Handling of URL Encoding (Hex Encoding)	888	449
HasMember	B	178	Improper Handling of Case Sensitivity	888	451
HasMember	B	179	Incorrect Behavior Order: Early Validation	888	454
HasMember	V	180	Incorrect Behavior Order: Validate Before Canonicalize	888	457
HasMember	V	181	Incorrect Behavior Order: Validate Before Filter	888	460
HasMember	B	182	Collapse of Data into Unsafe Value	888	462

Category-993: SFP Secondary Cluster: Incorrect Input Handling

Category ID : 993

Summary

This category identifies Software Fault Patterns (SFPs) within the Incorrect Input Handling cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	896	SFP Primary Cluster: Tainted Input	888	2406
HasMember	V	198	Use of Incorrect Byte Ordering	888	510
HasMember	C	228	Improper Handling of Syntactically Invalid Structure	888	575
HasMember	B	229	Improper Handling of Values	888	577
HasMember	V	230	Improper Handling of Missing Values	888	578
HasMember	V	231	Improper Handling of Extra Values	888	579
HasMember	V	232	Improper Handling of Undefined Values	888	580
HasMember	B	233	Improper Handling of Parameters	888	581
HasMember	V	234	Failure to Handle Missing Parameter	888	583
HasMember	V	235	Improper Handling of Extra Parameters	888	585
HasMember	V	236	Improper Handling of Undefined Parameters	888	586
HasMember	B	237	Improper Handling of Structural Elements	888	587
HasMember	V	238	Improper Handling of Incomplete Structural Elements	888	588
HasMember	V	239	Failure to Handle Incomplete Element	888	589
HasMember	B	240	Improper Handling of Inconsistent Structural Elements	888	590
HasMember	B	241	Improper Handling of Unexpected Data Type	888	591
HasMember	B	351	Insufficient Type Distinction	888	873
HasMember	B	354	Improper Validation of Integrity Check Value	888	883

Category-994: SFP Secondary Cluster: Tainted Input to Variable

Category ID : 994

Summary

This category identifies Software Fault Patterns (SFPs) within the Tainted Input to Variable cluster (SFP25).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	896	SFP Primary Cluster: Tainted Input	888	2406
HasMember	B	15	External Control of System or Configuration Setting	888	17
HasMember	C	20	Improper Input Validation	888	20

Nature	Type	ID	Name	V	Page
HasMember	B	454	External Initialization of Trusted Variables or Data Stores	888	1092
HasMember	V	496	Public Data Assigned to Private Array-Typed Field	888	1199
HasMember	B	502	Deserialization of Untrusted Data	888	1212
HasMember	V	566	Authorization Bypass Through User-Controlled SQL Primary Key	888	1294
HasMember	B	606	Unchecked Input for Loop Condition	888	1366
HasMember	V	616	Incomplete Identification of Uploaded File Variables (PHP)	888	1385

Category-995: SFP Secondary Cluster: Feature

Category ID : 995

Summary

This category identifies Software Fault Patterns (SFPs) within the Feature cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	906	SFP Primary Cluster: UI	888	2409
HasMember	B	447	Unimplemented or Unsupported Feature in UI	888	1082
HasMember	B	448	Obsolete Feature in UI	888	1083
HasMember	B	449	The UI Performs the Wrong Action	888	1084
HasMember	B	450	Multiple Interpretations of UI Input	888	1085
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	888	1087
HasMember	B	549	Missing Password Field Masking	888	1271
HasMember	C	655	Insufficient Psychological Acceptability	888	1450

Category-996: SFP Secondary Cluster: Security

Category ID : 996

Summary

This category identifies Software Fault Patterns (SFPs) within the Security cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	906	SFP Primary Cluster: UI	888	2409
HasMember	B	356	Product UI does not Warn User of Unsafe Actions	888	886
HasMember	B	357	Insufficient UI Warning of Dangerous Operations	888	887
HasMember	C	446	UI Discrepancy for Security Feature	888	1081

Category-997: SFP Secondary Cluster: Information Loss

Category ID : 997

Summary

This category identifies Software Fault Patterns (SFPs) within the Information Loss cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	906	SFP Primary Cluster: UI	888	2409
HasMember	C	221	Information Loss or Omission	888	563
HasMember	B	222	Truncation of Security-relevant Information	888	565
HasMember	B	223	Omission of Security-relevant Information	888	566
HasMember	B	224	Obscured Security-relevant Information by Alternate Name	888	568

Category-998: SFP Secondary Cluster: Glitch in Computation

Category ID : 998

Summary

This category identifies Software Fault Patterns (SFPs) within the Glitch in Computation cluster (SFP1).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	885	SFP Primary Cluster: Risky Values	888	2403
HasMember	B	128	Wrap-around Error	888	345
HasMember	B	190	Integer Overflow or Wraparound	888	478
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	888	487
HasMember	V	194	Unexpected Sign Extension	888	498
HasMember	V	195	Signed to Unsigned Conversion Error	888	501
HasMember	V	196	Unsigned to Signed Conversion Error	888	505
HasMember	B	197	Numeric Truncation Error	888	507
HasMember	B	369	Divide By Zero	888	920
HasMember	V	456	Missing Initialization of a Variable	888	1096
HasMember	V	457	Use of Uninitialized Variable	888	1102
HasMember	B	466	Return of Pointer Value Outside of Expected Range	888	1117
HasMember	B	468	Incorrect Pointer Scaling	888	1121
HasMember	B	475	Undefined Behavior for Input to API	888	1138
HasMember	B	480	Use of Incorrect Operator	888	1157
HasMember	V	481	Assigning instead of Comparing	888	1161
HasMember	V	486	Comparison of Classes by Name	888	1172
HasMember	B	562	Return of Stack Variable Address	888	1287
HasMember	B	570	Expression is Always False	888	1300
HasMember	B	571	Expression is Always True	888	1303
HasMember	V	579	J2EE Bad Practices: Non-serializable Object Stored in Session	888	1318
HasMember	V	587	Assignment of a Fixed Address to a Pointer	888	1330
HasMember	V	594	J2EE Framework: Saving Unserializable Objects to Disk	888	1341
HasMember	V	597	Use of Wrong Operator in String Comparison	888	1345
HasMember	B	628	Function Call with Incorrectly Specified Arguments	888	1407
HasMember	B	681	Incorrect Conversion between Numeric Types	888	1504
HasMember	V	683	Function Call With Incorrect Order of Arguments	888	1512

Nature	Type	ID	Name	V	Page
HasMember	V	685	Function Call With Incorrect Number of Arguments	888	1516
HasMember	V	686	Function Call With Incorrect Argument Type	888	1517
HasMember	V	688	Function Call With Incorrect Variable or Reference as Argument	888	1520
HasMember	C	704	Incorrect Type Conversion or Cast	888	1547
HasMember	V	768	Incorrect Short Circuit Evaluation	888	1620

Category-1001: SFP Secondary Cluster: Use of an Improper API

Category ID : 1001

Summary

This category identifies Software Fault Patterns (SFPs) within the Use of an Improper API cluster (SFP3).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	887	SFP Primary Cluster: API	888	2403
HasMember	V	111	Direct Use of Unsafe JNI	888	272
HasMember	C	227	7PK - API Abuse	888	2334
HasMember	B	242	Use of Inherently Dangerous Function	888	593
HasMember	V	245	J2EE Bad Practices: Direct Management of Connections	888	599
HasMember	V	246	J2EE Bad Practices: Direct Use of Sockets	888	601
HasMember	V	382	J2EE Bad Practices: Use of System.exit()	888	940
HasMember	V	383	J2EE Bad Practices: Direct Use of Threads	888	942
HasMember	B	432	Dangerous Signal Handler not Disabled During Sensitive Operations	888	1052
HasMember	B	439	Behavioral Change in New Version or Environment	888	1068
HasMember	B	440	Expected Behavior Violation	888	1069
HasMember	B	474	Use of Function with Inconsistent Implementations	888	1136
HasMember	B	477	Use of Obsolete Function	888	1146
HasMember	V	479	Signal Handler Use of a Non-reentrant Function	888	1154
HasMember	V	558	Use of getlogin() in Multithreaded Application	888	1281
HasMember	V	572	Call to Thread run() instead of start()	888	1305
HasMember	C	573	Improper Following of Specification by Caller	888	1307
HasMember	V	574	EJB Bad Practices: Use of Synchronization Primitives	888	1308
HasMember	V	575	EJB Bad Practices: Use of AWT Swing	888	1310
HasMember	V	576	EJB Bad Practices: Use of Java I/O	888	1312
HasMember	V	577	EJB Bad Practices: Use of Sockets	888	1314
HasMember	V	578	EJB Bad Practices: Use of Class Loader	888	1316
HasMember	B	586	Explicit Call to Finalize()	888	1329
HasMember	V	589	Call to Non-ubiquitous API	888	1333
HasMember	B	617	Reachable Assertion	888	1387
HasMember	B	676	Use of Potentially Dangerous Function	888	1498
HasMember	C	684	Incorrect Provision of Specified Functionality	888	1514
HasMember	B	695	Use of Low-Level Functionality	888	1533

Nature	Type	ID	Name	V	Page
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	888	1591

Category-1002: SFP Secondary Cluster: Unexpected Entry Points

Category ID : 1002

Summary

This category identifies Software Fault Patterns (SFPs) within the Unexpected Entry Points cluster.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	897	SFP Primary Cluster: Entry Points	888	2406
HasMember	B	489	Active Debug Code	888	1178
HasMember	V	491	Public cloneable() Method Without Final ('Object Hijack')	888	1181
HasMember	V	493	Critical Public Variable Without Final Modifier	888	1190
HasMember	V	500	Public Static Field Not Marked Final	888	1208
HasMember	V	531	Inclusion of Sensitive Information in Test Code	888	1249
HasMember	V	568	finalize() Method Without super.finalize()	888	1299
HasMember	V	580	clone() Method Without super.clone()	888	1319
HasMember	V	582	Array Declared Public, Final, and Static	888	1322
HasMember	V	583	finalize() Method Declared Public	888	1324
HasMember	V	608	Struts: Non-private Field in ActionForm Class	888	1369
HasMember	B	766	Critical Data Element Declared Public	888	1615

Category-1005: 7PK - Input Validation and Representation

Category ID : 1005

Summary

This category represents one of the phyla in the Seven Pernicious Kingdoms vulnerability classification. It includes weaknesses that exist when an application does not properly validate or represent input. According to the authors of the Seven Pernicious Kingdoms, "Input validation and representation problems are caused by metacharacters, alternate encodings and numeric representations. Security problems result from trusting input."

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	700	Seven Pernicious Kingdoms	700	2578
HasMember	C	20	Improper Input Validation	700	20
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	700	148
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	700	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	700	206
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	700	249

References

[REF-6]Katrina Tsipenyuk, Brian Chess and Gary McGraw. "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors". NIST Workshop on Software Security Assurance Tools Techniques and Metrics. 2005 November 7. NIST. < https://samate.nist.gov/SSATTM_Content/papers/Seven%20Pernicious%20Kingdoms%20-%20Taxonomy%20of%20Sw%20Security%20Errors%20-%20Tsipenyuk%20-%20Chess%20-%20McGraw.pdf >.

Category-1006: Bad Coding Practices

Category ID : 1006

Summary

Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. These weaknesses do not directly introduce a vulnerability, but indicate that the product has not been carefully developed or maintained. If a program is complex, difficult to maintain, not portable, or shows evidence of neglect, then there is a higher likelihood that weaknesses are buried in the code.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	358	Improperly Implemented Security Check for Standard	699	888
HasMember	B	360	Trust of System Event Data	699	894
HasMember	B	478	Missing Default Case in Multiple Condition Expression	699	1149
HasMember	B	487	Reliance on Package-level Scope	699	1175
HasMember	B	489	Active Debug Code	699	1178
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	699	1267
HasMember	B	561	Dead Code	699	1283
HasMember	B	562	Return of Stack Variable Address	699	1287
HasMember	B	563	Assignment to Variable without Use	699	1289
HasMember	V	581	Object Model Violation: Just One of Equals and Hashcode Defined	699	1321
HasMember	B	586	Explicit Call to Finalize()	699	1329
HasMember	V	605	Multiple Binds to the Same Port	699	1364
HasMember	B	628	Function Call with Incorrectly Specified Arguments	699	1407
HasMember	B	654	Reliance on a Single Factor in a Security Decision	699	1448
HasMember	C	656	Reliance on Security Through Obscurity	699	1452
HasMember	B	694	Use of Multiple Resources with Duplicate Identifier	699	1531
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	699	1723
HasMember	B	1041	Use of Redundant Code	699	1884
HasMember	B	1043	Data Element Aggregating an Excessively Large Number of Non-Primitive Elements	699	1887
HasMember	B	1044	Architecture with Number of Horizontal Layers Outside of Expected Range	699	1888
HasMember	B	1045	Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor	699	1889
HasMember	B	1046	Creation of Immutable Text Using String Concatenation	699	1890
HasMember	B	1048	Invokable Control Element with Large Number of Outward Calls	699	1892
HasMember	B	1049	Excessive Data Query Operations in a Large Data Table	699	1894

Nature	Type	ID	Name	V	Page
HasMember	B	1050	Excessive Platform Resource Consumption within a Loop	699	1895
HasMember	B	1063	Creation of Class Instance within a Static Code Block	699	1910
HasMember	B	1065	Runtime Resource Management Control Element in a Component Built to Run on Application Servers	699	1912
HasMember	B	1066	Missing Serialization Control Element	699	1913
HasMember	B	1067	Excessive Execution of Sequential Searches of Data Resource	699	1914
HasMember	B	1070	Serializable Data Element Containing non-Serializable Item Elements	699	1918
HasMember	B	1071	Empty Code Block	699	1919
HasMember	B	1072	Data Resource Access without Use of Connection Pooling	699	1921
HasMember	B	1073	Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses	699	1922
HasMember	B	1079	Parent Class without Virtual Destructor Method	699	1929
HasMember	B	1082	Class Instance Self Destruction Control Element	699	1931
HasMember	B	1084	Invokable Control Element with Excessive File or Data Access Operations	699	1933
HasMember	B	1085	Invokable Control Element with Excessive Volume of Commented-out Code	699	1934
HasMember	B	1087	Class with Virtual Method without a Virtual Destructor	699	1936
HasMember	B	1089	Large Data Table with Excessive Number of Indices	699	1938
HasMember	B	1092	Use of Same Invokable Control Element in Multiple Architectural Layers	699	1941
HasMember	B	1094	Excessive Index Range Scan for a Data Resource	699	1943
HasMember	B	1097	Persistent Storable Data Element without Associated Comparison Control Element	699	1946
HasMember	B	1098	Data Element containing Pointer Item without Proper Copy Control Element	699	1947
HasMember	B	1099	Inconsistent Naming Conventions for Identifiers	699	1948
HasMember	B	1101	Reliance on Runtime Component in Generated Code	699	1950
HasMember	B	1102	Reliance on Machine-Dependent Data Representation	699	1951
HasMember	B	1103	Use of Platform-Dependent Third Party Components	699	1952
HasMember	B	1104	Use of Unmaintained Third Party Components	699	1953
HasMember	B	1106	Insufficient Use of Symbolic Constants	699	1955
HasMember	B	1107	Insufficient Isolation of Symbolic Constant Definitions	699	1956
HasMember	B	1108	Excessive Reliance on Global Variables	699	1957
HasMember	B	1109	Use of Same Variable for Multiple Purposes	699	1958
HasMember	B	1113	Inappropriate Comment Style	699	1962
HasMember	B	1114	Inappropriate Whitespace Style	699	1963
HasMember	B	1115	Source Code Element without Standard Prologue	699	1963
HasMember	B	1116	Inaccurate Comments	699	1964
HasMember	B	1117	Callable with Insufficient Behavioral Summary	699	1966
HasMember	B	1126	Declaration of Variable with Unnecessarily Wide Scope	699	1975
HasMember	B	1127	Compilation with Insufficient Warnings or Errors	699	1976
HasMember	B	1235	Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations	699	2029

Category-1009: Audit

Category ID : 1009

Summary

Weaknesses in this category are related to the design and architecture of audit-based components of the system. Frequently these deal with logging user activities in order to identify attackers and modifications to the system. The weaknesses in this category could lead to a degradation of the quality of the audit capability if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	117	Improper Output Neutralization for Logs	1008	294
HasMember	B	223	Omission of Security-relevant Information	1008	566
HasMember	B	224	Obscured Security-relevant Information by Alternate Name	1008	568
HasMember	B	532	Insertion of Sensitive Information into Log File	1008	1250
HasMember	B	778	Insufficient Logging	1008	1647
HasMember	B	779	Logging of Excessive Data	1008	1651

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1010: Authenticate Actors

Category ID : 1010

Summary

Weaknesses in this category are related to the design and architecture of authentication components of the system. Frequently these deal with verifying the entity is indeed who it claims to be. The weaknesses in this category could lead to a degradation of the quality of authentication if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	V	258	Empty Password in Configuration File	1008	628
HasMember	V	259	Use of Hard-coded Password	1008	630
HasMember	B	262	Not Using Password Aging	1008	640
HasMember	B	263	Password Aging with Long Expiration	1008	643
HasMember	C	287	Improper Authentication	1008	699
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1008	707

Nature	Type	ID	Name	V	Page
HasMember	B	289	Authentication Bypass by Alternate Name	1008	710
HasMember	B	290	Authentication Bypass by Spoofing	1008	712
HasMember	V	291	Reliance on IP Address for Authentication	1008	715
HasMember	V	293	Using Referer Field for Authentication	1008	717
HasMember	B	294	Authentication Bypass by Capture-replay	1008	719
HasMember	B	301	Reflection Attack in an Authentication Protocol	1008	740
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	1008	742
HasMember	B	303	Incorrect Implementation of Authentication Algorithm	1008	744
HasMember	B	304	Missing Critical Step in Authentication	1008	745
HasMember	B	305	Authentication Bypass by Primary Weakness	1008	747
HasMember	B	306	Missing Authentication for Critical Function	1008	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	1008	754
HasMember	B	308	Use of Single-factor Authentication	1008	759
HasMember	B	322	Key Exchange without Entity Authentication	1008	795
HasMember	B	521	Weak Password Requirements	1008	1231
HasMember	V	593	Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created	1008	1339
HasMember	B	603	Use of Client-Side Authentication	1008	1363
HasMember	B	620	Unverified Password Change	1008	1392
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	1008	1418
HasMember	B	798	Use of Hard-coded Credentials	1008	1699
HasMember	B	836	Use of Password Hash Instead of Password for Authentication	1008	1770
HasMember	B	916	Use of Password Hash With Insufficient Computational Effort	1008	1822

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1011: Authorize Actors

Category ID : 1011

Summary

Weaknesses in this category are related to the design and architecture of a system's authorization components. Frequently these deal with enforcing that agents have the required permissions before performing certain operations, such as modifying data. The weaknesses in this category could lead to a degradation of quality of the authorization capability if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	15	External Control of System or Configuration Setting	1008	17
HasMember	C	114	Process Control	1008	283
HasMember	V	219	Storage of File with Sensitive Data Under Web Root	1008	560
HasMember	V	220	Storage of File With Sensitive Data Under FTP Root	1008	562
HasMember	B	266	Incorrect Privilege Assignment	1008	645
HasMember	B	267	Privilege Defined With Unsafe Actions	1008	648
HasMember	B	268	Privilege Chaining	1008	651
HasMember	C	269	Improper Privilege Management	1008	653
HasMember	B	270	Privilege Context Switching Error	1008	659
HasMember	C	271	Privilege Dropping / Lowering Errors	1008	660
HasMember	B	272	Least Privilege Violation	1008	663
HasMember	B	273	Improper Check for Dropped Privileges	1008	667
HasMember	B	274	Improper Handling of Insufficient Privileges	1008	670
HasMember	B	276	Incorrect Default Permissions	1008	672
HasMember	V	277	Insecure Inherited Permissions	1008	675
HasMember	V	279	Incorrect Execution-Assigned Permissions	1008	678
HasMember	B	280	Improper Handling of Insufficient Permissions or Privileges	1008	679
HasMember	B	281	Improper Preservation of Permissions	1008	681
HasMember	C	282	Improper Ownership Management	1008	683
HasMember	B	283	Unverified Ownership	1008	685
HasMember	P	284	Improper Access Control	1008	687
HasMember	C	285	Improper Authorization	1008	691
HasMember	C	286	Incorrect User Management	1008	698
HasMember	C	300	Channel Accessible by Non-Endpoint	1008	737
HasMember	B	341	Predictable from Observable State	1008	850
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	1008	889
HasMember	B	403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	1008	985
HasMember	B	419	Unprotected Primary Channel	1008	1024
HasMember	B	420	Unprotected Alternate Channel	1008	1025
HasMember	B	425	Direct Request ('Forced Browsing')	1008	1032
HasMember	B	426	Untrusted Search Path	1008	1035
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1008	1055
HasMember	V	527	Exposure of Version-Control Repository to an Unauthorized Control Sphere	1008	1245
HasMember	V	528	Exposure of Core Dump File to an Unauthorized Control Sphere	1008	1246
HasMember	V	529	Exposure of Access Control List Files to an Unauthorized Control Sphere	1008	1247
HasMember	V	530	Exposure of Backup File to an Unauthorized Control Sphere	1008	1248
HasMember	B	538	Insertion of Sensitive Information into Externally-Accessible File or Directory	1008	1257
HasMember	B	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	1008	1273
HasMember	B	552	Files or Directories Accessible to External Parties	1008	1274

Nature	Type	ID	Name	V	Page
HasMember	V	566	Authorization Bypass Through User-Controlled SQL Primary Key	1008	1294
HasMember	B	639	Authorization Bypass Through User-Controlled Key	1008	1415
HasMember	C	642	External Control of Critical State Data	1008	1422
HasMember	V	647	Use of Non-Canonical URL Paths for Authorization Decisions	1008	1435
HasMember	C	653	Improper Isolation or Compartmentalization	1008	1445
HasMember	C	656	Reliance on Security Through Obscurity	1008	1452
HasMember	C	668	Exposure of Resource to Wrong Sphere	1008	1478
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1008	1480
HasMember	C	671	Lack of Administrator Control over Security	1008	1487
HasMember	C	673	External Influence of Sphere Definition	1008	1492
HasMember	B	708	Incorrect Ownership Assignment	1008	1556
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1008	1559
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1008	1622
HasMember	V	782	Exposed IOCTL with Insufficient Access Control	1008	1657
HasMember	V	827	Improper Control of Document Type Definition	1008	1745
HasMember	C	862	Missing Authorization	1008	1789
HasMember	C	863	Incorrect Authorization	1008	1796
HasMember	B	921	Storage of Sensitive Data in a Mechanism without Access Control	1008	1834
HasMember	C	923	Improper Restriction of Communication Channel to Intended Endpoints	1008	1836
HasMember	B	939	Improper Authorization in Handler for Custom URL Scheme	1008	1849
HasMember	V	942	Permissive Cross-domain Policy with Untrusted Domains	1008	1857

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1012: Cross Cutting

Category ID : 1012

Summary

Weaknesses in this category are related to the design and architecture of multiple security tactics and how they affect a system. For example, information exposure can impact the Limit Access and Limit Exposure security tactics. The weaknesses in this category could lead to a degradation of the quality of many capabilities if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	208	Observable Timing Discrepancy	1008	537
HasMember	B	392	Missing Report of Error Condition	1008	958
HasMember	B	460	Improper Cleanup on Thrown Exception	1008	1109
HasMember	B	544	Missing Standardized Error Handling Mechanism	1008	1265
HasMember	C	602	Client-Side Enforcement of Server-Side Security	1008	1359
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1008	1544
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1008	1577
HasMember	V	784	Reliance on Cookies without Validation and Integrity Checking in a Security Decision	1008	1662
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1008	1723

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1013: Encrypt Data

Category ID : 1013

Summary

Weaknesses in this category are related to the design and architecture of data confidentiality in a system. Frequently these deal with the use of encryption libraries. The weaknesses in this category could lead to a degradation of the quality data encryption if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	256	Plaintext Storage of a Password	1008	622
HasMember	B	257	Storing Passwords in a Recoverable Format	1008	625
HasMember	B	260	Password in Configuration File	1008	636
HasMember	B	261	Weak Encoding for Password	1008	638
HasMember	C	311	Missing Encryption of Sensitive Data	1008	764
HasMember	B	312	Cleartext Storage of Sensitive Information	1008	771
HasMember	V	313	Cleartext Storage in a File or on Disk	1008	777
HasMember	V	314	Cleartext Storage in the Registry	1008	779
HasMember	V	315	Cleartext Storage of Sensitive Information in a Cookie	1008	781
HasMember	V	316	Cleartext Storage of Sensitive Information in Memory	1008	782
HasMember	V	317	Cleartext Storage of Sensitive Information in GUI	1008	784
HasMember	V	318	Cleartext Storage of Sensitive Information in Executable	1008	785
HasMember	B	319	Cleartext Transmission of Sensitive Information	1008	786
HasMember	V	321	Use of Hard-coded Cryptographic Key	1008	792
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	1008	797

Nature	Type	ID	Name	V	Page
HasMember	B	324	Use of a Key Past its Expiration Date	1008	799
HasMember	B	325	Missing Cryptographic Step	1008	801
HasMember	C	326	Inadequate Encryption Strength	1008	803
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1008	806
HasMember	B	328	Use of Weak Hash	1008	813
HasMember	C	330	Use of Insufficiently Random Values	1008	821
HasMember	B	331	Insufficient Entropy	1008	828
HasMember	V	332	Insufficient Entropy in PRNG	1008	830
HasMember	V	333	Improper Handling of Insufficient Entropy in TRNG	1008	832
HasMember	B	334	Small Space of Random Values	1008	834
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	1008	836
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1008	839
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1008	841
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	1008	844
HasMember	V	339	Small Seed Space in PRNG	1008	847
HasMember	B	347	Improper Verification of Cryptographic Signature	1008	864
HasMember	C	522	Insufficiently Protected Credentials	1008	1234
HasMember	B	523	Unprotected Transport of Credentials	1008	1239
HasMember	B	757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')	1008	1589
HasMember	V	759	Use of a One-Way Hash without a Salt	1008	1593
HasMember	V	760	Use of a One-Way Hash with a Predictable Salt	1008	1598
HasMember	V	780	Use of RSA Algorithm without OAEP	1008	1652
HasMember	C	922	Insecure Storage of Sensitive Information	1008	1835

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1014: Identify Actors

Category ID : 1014

Summary

Weaknesses in this category are related to the design and architecture of a system's identification management components. Frequently these deal with verifying that external agents provide inputs into the system. The weaknesses in this category could lead to a degradation of the quality of identification management if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	295	Improper Certificate Validation	1008	721
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	1008	726
HasMember	V	297	Improper Validation of Certificate with Host Mismatch	1008	729
HasMember	V	298	Improper Validation of Certificate Expiration	1008	733
HasMember	B	299	Improper Check for Certificate Revocation	1008	734
HasMember	C	345	Insufficient Verification of Data Authenticity	1008	858
HasMember	C	346	Origin Validation Error	1008	860
HasMember	V	370	Missing Check for Certificate Revocation after Initial Check	1008	924
HasMember	C	441	Unintended Proxy or Intermediary ('Confused Deputy')	1008	1072
HasMember	V	599	Missing Validation of OpenSSL Certificate	1008	1350
HasMember	B	940	Improper Verification of Source of a Communication Channel	1008	1852
HasMember	B	941	Incorrectly Specified Destination in a Communication Channel	1008	1855

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1015: Limit Access

Category ID : 1015

Summary

Weaknesses in this category are related to the design and architecture of system resources. Frequently these deal with restricting the amount of resources that are accessed by actors, such as memory, network connections, CPU or access points. The weaknesses in this category could lead to a degradation of the quality of authentication if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	73	External Control of File Name or Path	1008	133
HasMember	B	201	Insertion of Sensitive Information Into Sent Data	1008	521
HasMember	B	209	Generation of Error Message Containing Sensitive Information	1008	540
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	1008	551
HasMember	V	243	Creation of chroot Jail Without Changing Working Directory	1008	596
HasMember	B	250	Execution with Unnecessary Privileges	1008	606

Nature	Type	ID	Name	V	Page
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1008	1373
HasMember	B	611	Improper Restriction of XML External Entity Reference	1008	1376

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1016: Limit Exposure

Category ID : 1016

Summary

Weaknesses in this category are related to the design and architecture of the entry points to a system. Frequently these deal with minimizing the attack surface through designing the system with the least needed amount of entry points. The weaknesses in this category could lead to a degradation of a system's defenses if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	210	Self-generated Error Message Containing Sensitive Information	1008	546
HasMember	B	211	Externally-Generated Error Message Containing Sensitive Information	1008	548
HasMember	B	214	Invocation of Process Using Visible Sensitive Information	1008	556
HasMember	V	550	Server-generated Error Message Containing Sensitive Information	1008	1272
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1008	1750
HasMember	V	830	Inclusion of Web Functionality from an Untrusted Source	1008	1756

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1017: Lock Computer

Category ID : 1017

Summary

Weaknesses in this category are related to the design and architecture of a system's lockout mechanism. Frequently these deal with scenarios that take effect in case of multiple failed attempts to access a given resource. The weaknesses in this category could lead to a degradation of access to system assets if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	645	Overly Restrictive Account Lockout Mechanism	1008	1432

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1018: Manage User Sessions

Category ID : 1018

Summary

Weaknesses in this category are related to the design and architecture of session management. Frequently these deal with the information or status about each user and their access rights for the duration of multiple requests. The weaknesses in this category could lead to a degradation of the quality of session management if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	V	6	J2EE Misconfiguration: Insufficient Session-ID Length	1008	2
HasMember	C	384	Session Fixation	1008	943
HasMember	B	488	Exposure of Data Element to Wrong Session	1008	1176
HasMember	V	579	J2EE Bad Practices: Non-serializable Object Stored in Session	1008	1318
HasMember	B	613	Insufficient Session Expiration	1008	1380
HasMember	B	841	Improper Enforcement of Behavioral Workflow	1008	1781

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of

Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1019: Validate Inputs

Category ID : 1019

Summary

Weaknesses in this category are related to the design and architecture of a system's input validation components. Frequently these deal with sanitizing, neutralizing and validating any externally provided inputs to minimize malformed data from entering the system and preventing code injection in the input data. The weaknesses in this category could lead to a degradation of the quality of data flow in a system if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	C	20	Improper Input Validation	1008	20
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	1008	112
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1008	138
HasMember	C	75	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)	1008	145
HasMember	B	76	Improper Neutralization of Equivalent Special Elements	1008	146
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1008	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1008	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1008	168
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1008	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1008	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	1008	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	1008	220
HasMember	B	93	Improper Neutralization of CRLF Sequences ('CRLF Injection')	1008	222
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	1008	225
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	1008	232
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	1008	238
HasMember	V	97	Improper Neutralization of Server-Side Includes (SSI) Within a Web Page	1008	241
HasMember	V	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	1008	242

Nature	Type	ID	Name	V	Page
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	1008	249
HasMember	C	138	Improper Neutralization of Special Elements	1008	379
HasMember	V	150	Improper Neutralization of Escape, Meta, or Control Sequences	1008	400
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1008	868
HasMember	B	352	Cross-Site Request Forgery (CSRF)	1008	875
HasMember	B	472	External Control of Assumed-Immutable Web Parameter	1008	1131
HasMember	V	473	PHP External Variable Modification	1008	1134
HasMember	B	502	Deserialization of Untrusted Data	1008	1212
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1008	1353
HasMember	B	641	Improper Restriction of Names for Files and Other Resources	1008	1421
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1008	1428
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1008	1444
HasMember	C	790	Improper Filtering of Special Elements	1008	1687
HasMember	B	791	Incomplete Filtering of Special Elements	1008	1689
HasMember	V	792	Incomplete Filtering of One or More Instances of Special Elements	1008	1690
HasMember	V	793	Only Filtering One Instance of a Special Element	1008	1692
HasMember	V	794	Incomplete Filtering of Multiple Instances of Special Elements	1008	1693
HasMember	B	795	Only Filtering Special Elements at a Specified Location	1008	1694
HasMember	V	796	Only Filtering Special Elements Relative to a Marker	1008	1696
HasMember	V	797	Only Filtering Special Elements at an Absolute Position	1008	1698
HasMember	C	943	Improper Neutralization of Special Elements in Data Query Logic	1008	1860

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1020: Verify Message Integrity

Category ID : 1020

Summary

Weaknesses in this category are related to the design and architecture of a system's data integrity components. Frequently these deal with ensuring integrity of data, such as messages, resource files, deployment files, and configuration files. The weaknesses in this category could lead to a

degradation of data integrity quality if they are not addressed when designing or implementing a secure architecture.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1008	Architectural Concepts	1008	2598
HasMember	B	353	Missing Support for Integrity Check	1008	881
HasMember	B	354	Improper Validation of Integrity Check Value	1008	883
HasMember	B	390	Detection of Error Condition Without Action	1008	950
HasMember	B	391	Unchecked Error Condition	1008	955
HasMember	B	494	Download of Code Without Integrity Check	1008	1192
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	1008	1292
HasMember	B	649	Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking	1008	1439
HasMember	P	707	Improper Neutralization	1008	1554
HasMember	C	755	Improper Handling of Exceptional Conditions	1008	1585
HasMember	B	924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel	1008	1839

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.

[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Category-1027: OWASP Top Ten 2017 Category A1 - Injection

Category ID : 1027

Summary

Weaknesses in this category are related to the A1 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1026	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1026	155
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1026	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1026	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	1026	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	1026	220
HasMember	V	564	SQL Injection: Hibernate	1026	1290

Nature	Type	ID	Name	V	Page
HasMember	B	917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	1026	1827
HasMember	C	943	Improper Neutralization of Special Elements in Data Query Logic	1026	1860

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1028: OWASP Top Ten 2017 Category A2 - Broken Authentication

Category ID : 1028

Summary

Weaknesses in this category are related to the A2 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	B	256	Plaintext Storage of a Password	1026	622
HasMember	C	287	Improper Authentication	1026	699
HasMember	B	308	Use of Single-factor Authentication	1026	759
HasMember	B	384	Session Fixation	1026	943
HasMember	C	522	Insufficiently Protected Credentials	1026	1234
HasMember	B	523	Unprotected Transport of Credentials	1026	1239
HasMember	B	613	Insufficient Session Expiration	1026	1380
HasMember	B	620	Unverified Password Change	1026	1392
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	1026	1418

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1029: OWASP Top Ten 2017 Category A3 - Sensitive Data Exposure

Category ID : 1029

Summary

Weaknesses in this category are related to the A3 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	V	220	Storage of File With Sensitive Data Under FTP Root	1026	562
HasMember	B	295	Improper Certificate Validation	1026	721
HasMember	C	311	Missing Encryption of Sensitive Data	1026	764
HasMember	B	312	Cleartext Storage of Sensitive Information	1026	771

Nature	Type	ID	Name	V	Page
HasMember	B	319	Cleartext Transmission of Sensitive Information	1026	786
HasMember	C	320	Key Management Errors	1026	2340
HasMember	B	325	Missing Cryptographic Step	1026	801
HasMember	C	326	Inadequate Encryption Strength	1026	803
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1026	806
HasMember	B	328	Use of Weak Hash	1026	813
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	1026	889

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1030: OWASP Top Ten 2017 Category A4 - XML External Entities (XXE)

Category ID : 1030

Summary

Weaknesses in this category are related to the A4 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	B	611	Improper Restriction of XML External Entity Reference	1026	1376
HasMember	B	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	1026	1642

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1031: OWASP Top Ten 2017 Category A5 - Broken Access Control

Category ID : 1031

Summary

Weaknesses in this category are related to the A5 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1026	33
HasMember	P	284	Improper Access Control	1026	687
HasMember	C	285	Improper Authorization	1026	691
HasMember	B	425	Direct Request ('Forced Browsing')	1026	1032
HasMember	B	639	Authorization Bypass Through User-Controlled Key	1026	1415

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1032: OWASP Top Ten 2017 Category A6 - Security Misconfiguration

Category ID : 1032

Summary

Weaknesses in this category are related to the A6 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
MemberOf	C	1349	OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration	1344	2514
HasMember	C	16	Configuration	1026	2330
HasMember	B	209	Generation of Error Message Containing Sensitive Information	1026	540
HasMember	V	548	Exposure of Information Through Directory Listing	1026	1269

Notes

Relationship

While the OWASP document maps to CWE-2 and CWE-388, these are not appropriate for mapping, as they are high-level categories that are only intended for the Seven Pernicious Kingdoms view (CWE-700).

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1033: OWASP Top Ten 2017 Category A7 - Cross-Site Scripting (XSS)

Category ID : 1033

Summary

Weaknesses in this category are related to the A7 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1026	168

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1034: OWASP Top Ten 2017 Category A8 - Insecure Deserialization

Category ID : 1034

Summary

Weaknesses in this category are related to the A8 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	B	502	Deserialization of Untrusted Data	1026	1212

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1035: OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities

Category ID : 1035

Summary

Weaknesses in this category are related to the A9 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
MemberOf	C	1352	OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components	1344	2515

Notes

Relationship

This is an unusual category. CWE does not cover the limitations of human processes and procedures that cannot be described in terms of a specific technical weakness as resident in the code, architecture, or configuration of the software. Since "known vulnerabilities" can arise from any kind of weakness, it is not possible to map this OWASP category to other CWE entries, since it would effectively require mapping this category to ALL weaknesses.

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1036: OWASP Top Ten 2017 Category A10 - Insufficient Logging & Monitoring

Category ID : 1036

Summary

Weaknesses in this category are related to the A10 category in the OWASP Top Ten 2017.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1026	Weaknesses in OWASP Top Ten (2017)	1026	2599
HasMember	B	223	Omission of Security-relevant Information	1026	566
HasMember	B	778	Insufficient Logging	1026	1647

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Category-1129: CISQ Quality Measures (2016) - Reliability

Category ID : 1129

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Reliability, as documented in 2016 with the Automated Source Code CISQ Reliability Measure (ASCRM) Specification 1.0. Presence of these weaknesses could reduce the reliability of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1128	CISQ Quality Measures (2016)	1128	2602
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1128	310
HasMember	B	252	Unchecked Return Value	1128	613
HasMember	B	396	Declaration of Catch for Generic Exception	1128	966
HasMember	B	397	Declaration of Throws for Generic Exception	1128	968
HasMember	V	456	Missing Initialization of a Variable	1128	1096
HasMember	C	674	Uncontrolled Recursion	1128	1493
HasMember	C	704	Incorrect Type Conversion or Cast	1128	1547
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1128	1632
HasMember	B	788	Access of Memory Location After End of Buffer	1128	1678
HasMember	B	1045	Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor	1128	1889
HasMember	B	1047	Modules with Circular Dependencies	1128	1891
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1128	1896
HasMember	B	1056	Invokable Control Element with Variadic Parameters	1128	1901
HasMember	B	1058	Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element	1128	1903
HasMember	B	1062	Parent Class with References to Child Class	1128	1909
HasMember	B	1065	Runtime Resource Management Control Element in a Component Built to Run on Application Servers	1128	1912
HasMember	B	1066	Missing Serialization Control Element	1128	1913
HasMember	V	1069	Empty Exception Block	1128	1916
HasMember	B	1070	Serializable Data Element Containing non-Serializable Item Elements	1128	1918
HasMember	V	1077	Floating Point Comparison with Incorrect Operator	1128	1926
HasMember	B	1079	Parent Class without Virtual Destructor Method	1128	1929
HasMember	B	1082	Class Instance Self Destruction Control Element	1128	1931
HasMember	B	1083	Data Access from Outside Expected Data Manager Component	1128	1932

Nature	Type	ID	Name	V	Page
HasMember	B	1087	Class with Virtual Method without a Virtual Destructor	1128	1936
HasMember	B	1088	Synchronous Access of Remote Resource without Timeout	1128	1937
HasMember	V	1096	Singleton Class Instance Creation without Proper Locking or Synchronization	1128	1945
HasMember	B	1097	Persistent Storable Data Element without Associated Comparison Control Element	1128	1946
HasMember	B	1098	Data Element containing Pointer Item without Proper Copy Control Element	1128	1947

References

[REF-961]Object Management Group (OMG). "Automated Source Code Reliability Measure (ASCRM)". 2016 January. < http://www.omg.org/spec/ASCRM/1.0/ >.

[REF-968]Consortium for Information & Software Quality (CISQ). "Automated Quality Characteristic Measures". 2016. < http://it-cisq.org/standards/automated-quality-characteristic-measures/ >.

Category-1130: CISQ Quality Measures (2016) - Maintainability

Category ID : 1130

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Maintainability, as documented in 2016 with the Automated Source Code Maintainability Measure (ASCMM) Specification 1.0. Presence of these weaknesses could reduce the maintainability of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1128	CISQ Quality Measures (2016)	1128	2602
HasMember	B	561	Dead Code	1128	1283
HasMember	B	766	Critical Data Element Declared Public	1128	1615
HasMember	B	1041	Use of Redundant Code	1128	1884
HasMember	B	1044	Architecture with Number of Horizontal Layers Outside of Expected Range	1128	1888
HasMember	B	1047	Modules with Circular Dependencies	1128	1891
HasMember	B	1048	Invokable Control Element with Large Number of Outward Calls	1128	1892
HasMember	B	1052	Excessive Use of Hard-Coded Literals in Initialization	1128	1897
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer	1128	1899
HasMember	B	1055	Multiple Inheritance from Concrete Classes	1128	1900
HasMember	B	1064	Invokable Control Element with Signature Containing an Excessive Number of Parameters	1128	1911
HasMember	B	1074	Class with Excessively Deep Inheritance	1128	1923
HasMember	B	1075	Unconditional Control Flow Transfer outside of Switch Block	1128	1924
HasMember	B	1080	Source Code File with Excessive Number of Lines of Code	1128	1930
HasMember	B	1084	Invokable Control Element with Excessive File or Data Access Operations	1128	1933

Nature	Type	ID	Name	V	Page
HasMember	B	1085	Invokable Control Element with Excessive Volume of Commented-out Code	1128	1934
HasMember	B	1086	Class with Excessive Number of Child Classes	1128	1935
HasMember	B	1090	Method Containing Access of a Member Element from Another Class	1128	1939
HasMember	B	1092	Use of Same Invokable Control Element in Multiple Architectural Layers	1128	1941
HasMember	B	1095	Loop Condition Value Update within the Loop	1128	1944
HasMember	B	1121	Excessive McCabe Cyclomatic Complexity	1128	1970

References

[REF-960]Object Management Group (OMG). "Automated Source Code Maintainability Measure (ASCMM)". 2016 January. < https://www.omg.org/spec/ASCMM/ >.2023-04-07.

[REF-968]Consortium for Information & Software Quality (CISQ). "Automated Quality Characteristic Measures". 2016. < http://it-cisq.org/standards/automated-quality-characteristic-measures/ >.

Category-1131: CISQ Quality Measures (2016) - Security

Category ID : 1131

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Security, as documented in 2016 with the Automated Source Code Security Measure (ASCSM) Specification 1.0. Presence of these weaknesses could reduce the security of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1128	CISQ Quality Measures (2016)	1128	2602
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1128	33
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1128	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1128	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1128	206
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	1128	249
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1128	310
HasMember	V	129	Improper Validation of Array Index	1128	347
HasMember	B	134	Use of Externally-Controlled Format String	1128	371
HasMember	B	252	Unchecked Return Value	1128	613
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1128	806
HasMember	B	396	Declaration of Catch for Generic Exception	1128	966
HasMember	B	397	Declaration of Throws for Generic Exception	1128	968
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1128	1055
HasMember	V	456	Missing Initialization of a Variable	1128	1096
HasMember	B	606	Unchecked Input for Loop Condition	1128	1366
HasMember	C	667	Improper Locking	1128	1472

Nature	Type	ID	Name	V	Page
HasMember	C	672	Operation on a Resource after Expiration or Release	1128	1488
HasMember	B	681	Incorrect Conversion between Numeric Types	1128	1504
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1128	1632
HasMember	V	789	Memory Allocation with Excessive Size Value	1128	1683
HasMember	B	798	Use of Hard-coded Credentials	1128	1699
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1128	1766

References

[REF-962]Object Management Group (OMG). "Automated Source Code Security Measure (ASCSM)". 2016 January. < http://www.omg.org/spec/ASCSM/1.0/ >.

[REF-968]Consortium for Information & Software Quality (CISQ). "Automated Quality Characteristic Measures". 2016. < http://it-cisq.org/standards/automated-quality-characteristic-measures/ >.

Category-1132: CISQ Quality Measures (2016) - Performance Efficiency

Category ID : 1132

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Performance Efficiency, as documented in 2016 with the Automated Source Code Performance Efficiency Measure (ASCPEM) Specification 1.0. Presence of these weaknesses could reduce the performance efficiency of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1128	CISQ Quality Measures (2016)	1128	2602
HasMember	V	1042	Static Member Data Element outside of a Singleton Class Element	1128	1886
HasMember	B	1043	Data Element Aggregating an Excessively Large Number of Non-Primitive Elements	1128	1887
HasMember	B	1046	Creation of Immutable Text Using String Concatenation	1128	1890
HasMember	B	1049	Excessive Data Query Operations in a Large Data Table	1128	1894
HasMember	B	1050	Excessive Platform Resource Consumption within a Loop	1128	1895
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component	1128	1902
HasMember	B	1060	Excessive Number of Inefficient Server-Side Data Accesses	1128	1906
HasMember	B	1063	Creation of Class Instance within a Static Code Block	1128	1910
HasMember	B	1067	Excessive Execution of Sequential Searches of Data Resource	1128	1914
HasMember	B	1072	Data Resource Access without Use of Connection Pooling	1128	1921
HasMember	B	1073	Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses	1128	1922
HasMember	B	1089	Large Data Table with Excessive Number of Indices	1128	1938
HasMember	B	1091	Use of Object without Invoking Destructor Method	1128	1940
HasMember	B	1094	Excessive Index Range Scan for a Data Resource	1128	1943

References

[REF-959]Object Management Group (OMG). "Automated Source Code Performance Efficiency Measure (ASCPEM)". 2016 January. < https://www.omg.org/spec/ASCPEM/ >.2023-04-07.

[REF-968]Consortium for Information & Software Quality (CISQ). "Automated Quality Characteristic Measures". 2016. < http://it-cisq.org/standards/automated-quality-characteristic-measures/ >.

Category-1134: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 00. Input Validation and Data Sanitization (IDS)

Category ID : 1134

Summary

Weaknesses in this category are related to the rules and recommendations in the Input Validation and Data Sanitization (IDS) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1133	155
HasMember	C	116	Improper Encoding or Escaping of Output	1133	287
HasMember	B	117	Improper Output Neutralization for Logs	1133	294
HasMember	B	134	Use of Externally-Controlled Format String	1133	371
HasMember	V	144	Improper Neutralization of Line Delimiters	1133	389
HasMember	V	150	Improper Neutralization of Escape, Meta, or Control Sequences	1133	400
HasMember	V	180	Incorrect Behavior Order: Validate Before Canonicalize	1133	457
HasMember	B	182	Collapse of Data into Unsafe Value	1133	462
HasMember	B	289	Authentication Bypass by Alternate Name	1133	710
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	1133	1004

References

[REF-814]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 00. Input Validation and Data Sanitization (IDS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487865 >.

[REF-996]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 00. Input Validation and Data Sanitization (IDS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487337 >.

Category-1135: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 01. Declarations and Initialization (DCL)

Category ID : 1135

Summary

Weaknesses in this category are related to the rules and recommendations in the Declarations and Initialization (DCL) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	C	665	Improper Initialization	1133	1465

References

[REF-815]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 01. Declarations and Initialization (DCL)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487858 >.

[REF-997]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 01. Declarations and Initialization (DCL)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487329 >.

Category-1136: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 02. Expressions (EXP)

Category ID : 1136

Summary

Weaknesses in this category are related to the rules and recommendations in the Expressions (EXP) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	252	Unchecked Return Value	1133	613
HasMember	B	476	NULL Pointer Dereference	1133	1139
HasMember	V	595	Comparison of Object References Instead of Object Contents	1133	1342
HasMember	V	597	Use of Wrong Operator in String Comparison	1133	1345

References

[REF-816]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 02. Expressions (EXP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487704 >.

[REF-998]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 02. Expressions (EXP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487331 >.

Category-1137: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 03. Numeric Types and Operations (NUM)

Category ID : 1137

Summary

Weaknesses in this category are related to the rules and recommendations in the Numeric Types and Operations (NUM) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	190	Integer Overflow or Wraparound	1133	478
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	1133	487
HasMember	B	197	Numeric Truncation Error	1133	507
HasMember	B	369	Divide By Zero	1133	920
HasMember	B	681	Incorrect Conversion between Numeric Types	1133	1504
HasMember	P	682	Incorrect Calculation	1133	1507

References

[REF-817]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 03. Numeric Types and Operations (NUM)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487628 >.

[REF-999]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 03. Numeric Types and Operations (NUM)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487335 >.

Category-1138: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 04. Characters and Strings (STR)

Category ID : 1138

Summary

Weaknesses in this category are related to the rules and recommendations in the Characters and Strings (STR) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	838	Inappropriate Encoding for Output Context	1133	1773

References

[REF-971]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 04. Characters and Strings (STR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487607 >.

[REF-1000]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 04. Characters and Strings (STR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487333 >.

Category-1139: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 05. Object Orientation (OBJ)

Category ID : 1139

Summary

Weaknesses in this category are related to the rules and recommendations in the Object Orientation (OBJ) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	374	Passing Mutable Objects to an Untrusted Method	1133	927
HasMember	B	375	Returning a Mutable Object to an Untrusted Caller	1133	930
HasMember	V	486	Comparison of Classes by Name	1133	1172
HasMember	V	491	Public cloneable() Method Without Final ('Object Hijack')	1133	1181
HasMember	V	492	Use of Inner Class Containing Sensitive Data	1133	1183
HasMember	V	498	Cloneable Class Containing Sensitive Information	1133	1204
HasMember	V	500	Public Static Field Not Marked Final	1133	1208
HasMember	B	766	Critical Data Element Declared Public	1133	1615

References

[REF-818]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 05. Object Orientation (OBJ)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487715 >.

[REF-1001]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 05. Object Orientation (OBJ)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487353 >.

Category-1140: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 06. Methods (MET)

Category ID : 1140

Summary

Weaknesses in this category are related to the rules and recommendations in the Methods (MET) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	V	568	finalize() Method Without super.finalize()	1133	1299
HasMember	C	573	Improper Following of Specification by Caller	1133	1307
HasMember	V	581	Object Model Violation: Just One of Equals and Hashcode Defined	1133	1321
HasMember	V	583	finalize() Method Declared Public	1133	1324
HasMember	B	586	Explicit Call to Finalize()	1133	1329
HasMember	V	589	Call to Non-ubiquitous API	1133	1333
HasMember	B	617	Reachable Assertion	1133	1387
HasMember	P	697	Incorrect Comparison	1133	1538

References

[REF-819]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 06. Methods (MET)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487441 >.

[REF-1002]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 06. Methods (MET)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487336 >.

Category-1141: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 07. Exceptional Behavior (ERR)

Category ID : 1141

Summary

Weaknesses in this category are related to the rules and recommendations in the Exceptional Behavior (ERR) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	248	Uncaught Exception	1133	603
HasMember	V	382	J2EE Bad Practices: Use of System.exit()	1133	940
HasMember	B	397	Declaration of Throws for Generic Exception	1133	968
HasMember	B	459	Incomplete Cleanup	1133	1106
HasMember	B	460	Improper Cleanup on Thrown Exception	1133	1109
HasMember	B	584	Return Inside Finally Block	1133	1325
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1133	1544
HasMember	C	705	Incorrect Control Flow Scoping	1133	1550
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1133	1577

References

[REF-820]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 07. Exceptional Behavior (ERR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487665 >.

[REF-1003]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 07. Exceptional Behavior (ERR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487338 >.

Category-1142: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 08. Visibility and Atomicity (VNA)

Category ID : 1142

Summary

Weaknesses in this category are related to the rules and recommendations in the Visibility and Atomicity (VNA) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1133	895

Nature	Type	ID	Name	V	Page
HasMember	B	366	Race Condition within a Thread	1133	910
HasMember	B	413	Improper Resource Locking	1133	1010
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	1133	1296
HasMember	C	662	Improper Synchronization	1133	1457
HasMember	C	667	Improper Locking	1133	1472

References

[REF-821]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 08. Visibility and Atomicity (VNA)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487824 >.

Category-1143: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 09. Locking (LCK)

Category ID : 1143

Summary

Weaknesses in this category are related to the rules and recommendations in the Locking (LCK) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	412	Unrestricted Externally Accessible Lock	1133	1007
HasMember	B	609	Double-Checked Locking	1133	1371
HasMember	C	667	Improper Locking	1133	1472
HasMember	B	820	Missing Synchronization	1133	1729

References

[REF-822]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 09. Locking (LCK)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487666 >.

Category-1144: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 10. Thread APIs (THI)

Category ID : 1144

Summary

Weaknesses in this category are related to the rules and recommendations in the Thread APIs (THI) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	V	572	Call to Thread run() instead of start()	1133	1305

References

[REF-823]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 10. Thread APIs (THI)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487735 >.

Category-1145: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 11. Thread Pools (TPS)

Category ID : 1145

Summary

Weaknesses in this category are related to the rules and recommendations in the Thread Pools (TPS) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	392	Missing Report of Error Condition	1133	958
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	1133	993
HasMember	B	410	Insufficient Resource Pool	1133	1005

References

[REF-824]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 11. Thread Pools (TPS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487728 >.

Category-1146: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 12. Thread-Safety Miscellaneous (TSM)

Category ID : 1146

Summary

Weaknesses in this category are related to the rules and recommendations in the Thread-Safety Miscellaneous (TSM) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603

References

[REF-825]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 12. Thread-Safety Miscellaneous (TSM)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487731 >.

Category-1147: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 13. Input Output (FIO)

Category ID : 1147

Summary

Weaknesses in this category are related to the rules and recommendations in the Input Output (FIO) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	V	67	Improper Handling of Windows Device Names	1133	127
HasMember	V	180	Incorrect Behavior Order: Validate Before Canonicalize	1133	457
HasMember	V	198	Use of Incorrect Byte Ordering	1133	510
HasMember	B	276	Incorrect Default Permissions	1133	672
HasMember	V	279	Incorrect Execution-Assigned Permissions	1133	678
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	1133	889
HasMember	C	377	Insecure Temporary File	1133	932
HasMember	C	404	Improper Resource Shutdown or Release	1133	987
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	1133	993
HasMember	B	459	Incomplete Cleanup	1133	1106
HasMember	B	532	Insertion of Sensitive Information into Log File	1133	1250
HasMember	V	647	Use of Non-Canonical URL Paths for Authorization Decisions	1133	1435
HasMember	C	705	Incorrect Control Flow Scoping	1133	1550
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1133	1559
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1133	1622

References

[REF-826]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 13. Input Output (FIO)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487725 >.

[REF-1004]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 13. Input Output (FIO)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487330 >.

Category-1148: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 14. Serialization (SER)

Category ID : 1148

Summary

Weaknesses in this category are related to the rules and recommendations in the Serialization (SER) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	319	Cleartext Transmission of Sensitive Information	1133	786
HasMember	C	400	Uncontrolled Resource Consumption	1133	971

Nature	Type	ID	Name	V	Page
HasMember	V	499	Serializable Class Containing Sensitive Data	1133	1206
HasMember	B	502	Deserialization of Untrusted Data	1133	1212
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1133	1622

References

[REF-827]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 14. Serialization (SER)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487787 >.

Category-1149: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 15. Platform Security (SEC)

Category ID : 1149

Summary

Weaknesses in this category are related to the rules and recommendations in the Platform Security (SEC) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	266	Incorrect Privilege Assignment	1133	645
HasMember	B	272	Least Privilege Violation	1133	663
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1133	1559

References

[REF-828]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 15. Platform Security (SEC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487683 >.

[REF-1005]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 15. Platform Security (SEC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487332 >.

Category-1150: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 16. Runtime Environment (ENV)

Category ID : 1150

Summary

Weaknesses in this category are related to the rules and recommendations in the Runtime Environment (ENV) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1133	868

Nature	Type	ID	Name	V	Page
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1133	1559

References

[REF-829]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 16. Runtime Environment (ENV)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487764 >.

Category-1151: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 17. Java Native Interface (JNI)

Category ID : 1151

Summary

Weaknesses in this category are related to the rules and recommendations in the Java Native Interface (JNI) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	V	111	Direct Use of Unsafe JNI	1133	272

References

[REF-972]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 17. Java Native Interface (JNI)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487346 >.

Category-1152: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 49. Miscellaneous (MSC)

Category ID : 1152

Summary

Weaknesses in this category are related to the rules and recommendations in the Miscellaneous (MSC) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603
HasMember	V	259	Use of Hard-coded Password	1133	630
HasMember	C	311	Missing Encryption of Sensitive Data	1133	764
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1133	806
HasMember	C	330	Use of Insufficiently Random Values	1133	821
HasMember	V	332	Insufficient Entropy in PRNG	1133	830
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1133	839
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1133	841

Nature	Type	ID	Name	V	Page
HasMember	C	400	Uncontrolled Resource Consumption	1133	971
HasMember	V	401	Missing Release of Memory after Effective Lifetime	1133	980
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1133	1622
HasMember	B	798	Use of Hard-coded Credentials	1133	1699

References

[REF-830]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 49. Miscellaneous (MSC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487686 >.

[REF-1006]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 49. Miscellaneous (MSC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487351 >.

Category-1153: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 50. Android (DRD)

Category ID : 1153

Summary

Weaknesses in this category are related to the rules and recommendations in the Android (DRD) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603

References

[REF-973]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rule 50. Android (DRD)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487375 >.

Category-1155: SEI CERT C Coding Standard - Guidelines 01. Preprocessor (PRE)

Category ID : 1155

Summary

Weaknesses in this category are related to the rules and recommendations in the Preprocessor (PRE) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604

References

[REF-599]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 01. Preprocessor (PRE)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152276 >.

[REF-979]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 01. Preprocessor (PRE)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151965 >.

Category-1156: SEI CERT C Coding Standard - Guidelines 02. Declarations and Initialization (DCL)

Category ID : 1156

Summary

Weaknesses in this category are related to the rules and recommendations in the Declarations and Initialization (DCL) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	562	Return of Stack Variable Address	1154	1287

References

[REF-600]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 02. Declarations and Initialization (DCL)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152215 >.

[REF-980]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 02. Declarations and Initialization (DCL)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151966 >.

Category-1157: SEI CERT C Coding Standard - Guidelines 03. Expressions (EXP)

Category ID : 1157

Summary

Weaknesses in this category are related to the rules and recommendations in the Expressions (EXP) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1154	299
HasMember	B	125	Out-of-bounds Read	1154	336
HasMember	B	476	NULL Pointer Dereference	1154	1139
HasMember	B	480	Use of Incorrect Operator	1154	1157
HasMember	V	481	Assigning instead of Comparing	1154	1161
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1154	1407
HasMember	V	685	Function Call With Incorrect Number of Arguments	1154	1516
HasMember	V	686	Function Call With Incorrect Argument Type	1154	1517
HasMember	∞	690	Unchecked Return Value to NULL Pointer Dereference	1154	1523

Nature	Type	ID	Name	V	Page
HasMember	C	704	Incorrect Type Conversion or Cast	1154	1547
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591
HasMember	B	843	Access of Resource Using Incompatible Type ('Type Confusion')	1154	1785
HasMember	B	908	Use of Uninitialized Resource	1154	1802

References

[REF-601]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 03. Expressions (EXP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152200 >.

[REF-981]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 03. Expressions (EXP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151976 >.

Category-1158: SEI CERT C Coding Standard - Guidelines 04. Integers (INT)

Category ID : 1158

Summary

Weaknesses in this category are related to the rules and recommendations in the Integers (INT) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	131	Incorrect Calculation of Buffer Size	1154	361
HasMember	B	190	Integer Overflow or Wraparound	1154	478
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	1154	487
HasMember	V	192	Integer Coercion Error	1154	489
HasMember	V	194	Unexpected Sign Extension	1154	498
HasMember	V	195	Signed to Unsigned Conversion Error	1154	501
HasMember	B	197	Numeric Truncation Error	1154	507
HasMember	B	369	Divide By Zero	1154	920
HasMember	V	587	Assignment of a Fixed Address to a Pointer	1154	1330
HasMember	∞	680	Integer Overflow to Buffer Overflow	1154	1502
HasMember	B	681	Incorrect Conversion between Numeric Types	1154	1504
HasMember	P	682	Incorrect Calculation	1154	1507
HasMember	C	704	Incorrect Type Conversion or Cast	1154	1547
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591

References

[REF-602]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 04. Integers (INT)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152052 >.

[REF-982]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec. 04. Integers (INT)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151979 >.

Category-1159: SEI CERT C Coding Standard - Guidelines 05. Floating Point (FLP)

Category ID : 1159

Summary

Weaknesses in this category are related to the rules and recommendations in the Floating Point (FLP) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	197	Numeric Truncation Error	1154	507
HasMember	B	391	Unchecked Error Condition	1154	955
HasMember	B	681	Incorrect Conversion between Numeric Types	1154	1504
HasMember	P	682	Incorrect Calculation	1154	1507

References

[REF-603]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 05. Floating Point (FLP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152181 >.

[REF-983]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 05. Floating Point (FLP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151969 >.

Category-1160: SEI CERT C Coding Standard - Guidelines 06. Arrays (ARR)

Category ID : 1160

Summary

Weaknesses in this category are related to the rules and recommendations in the Arrays (ARR) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1154	299
HasMember	V	121	Stack-based Buffer Overflow	1154	320
HasMember	B	123	Write-what-where Condition	1154	329
HasMember	B	125	Out-of-bounds Read	1154	336
HasMember	V	129	Improper Validation of Array Index	1154	347
HasMember	B	468	Incorrect Pointer Scaling	1154	1121
HasMember	B	469	Use of Pointer Subtraction to Determine Size	1154	1123
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591
HasMember	B	786	Access of Memory Location Before Start of Buffer	1154	1666
HasMember	B	805	Buffer Access with Incorrect Length Value	1154	1711

References

[REF-604]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 06. Arrays (ARR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152051 >.

[REF-984]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 06. Arrays (ARR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151972 >.

Category-1161: SEI CERT C Coding Standard - Guidelines 07. Characters and Strings (STR)

Category ID : 1161

Summary

Weaknesses in this category are related to the rules and recommendations in the Characters and Strings (STR) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1154	299
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1154	310
HasMember	V	121	Stack-based Buffer Overflow	1154	320
HasMember	V	122	Heap-based Buffer Overflow	1154	324
HasMember	B	123	Write-what-where Condition	1154	329
HasMember	B	125	Out-of-bounds Read	1154	336
HasMember	B	170	Improper Null Termination	1154	434
HasMember	B	676	Use of Potentially Dangerous Function	1154	1498
HasMember	C	704	Incorrect Type Conversion or Cast	1154	1547

References

[REF-605]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 07. Characters and Strings (STR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152038 >.

[REF-985]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 07. Characters and Strings (STR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151974 >.

Category-1162: SEI CERT C Coding Standard - Guidelines 08. Memory Management (MEM)

Category ID : 1162

Summary

Weaknesses in this category are related to the rules and recommendations in the Memory Management (MEM) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	131	Incorrect Calculation of Buffer Size	1154	361
HasMember	B	190	Integer Overflow or Wraparound	1154	478
HasMember	V	401	Missing Release of Memory after Effective Lifetime	1154	980
HasMember	C	404	Improper Resource Shutdown or Release	1154	987
HasMember	V	415	Double Free	1154	1015
HasMember	V	416	Use After Free	1154	1019
HasMember	B	459	Incomplete Cleanup	1154	1106
HasMember	V	467	Use of sizeof() on a Pointer Type	1154	1118
HasMember	V	590	Free of Memory not on the Heap	1154	1335
HasMember	C	666	Operation on Resource in Wrong Phase of Lifetime	1154	1471
HasMember	C	672	Operation on a Resource after Expiration or Release	1154	1488
HasMember	⛓	680	Integer Overflow to Buffer Overflow	1154	1502
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591
HasMember	B	771	Missing Reference to Active Allocated Resource	1154	1631
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1154	1632
HasMember	V	789	Memory Allocation with Excessive Size Value	1154	1683

References

[REF-606]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 08. Memory Management (MEM)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152142 >.

[REF-986]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec. 08. Memory Management (MEM)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151930 >.

Category-1163: SEI CERT C Coding Standard - Guidelines 09. Input Output (FIO)

Category ID : 1163

Summary

Weaknesses in this category are related to the rules and recommendations in the Input Output (FIO) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	C	20	Improper Input Validation	1154	20
HasMember	V	67	Improper Handling of Windows Device Names	1154	127
HasMember	B	134	Use of Externally-Controlled Format String	1154	371
HasMember	B	197	Numeric Truncation Error	1154	507
HasMember	B	241	Improper Handling of Unexpected Data Type	1154	591
HasMember	C	404	Improper Resource Shutdown or Release	1154	987
HasMember	B	459	Incomplete Cleanup	1154	1106
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1154	1463

Nature	Type	ID	Name	V	Page
HasMember	C	666	Operation on Resource in Wrong Phase of Lifetime	1154	1471
HasMember	C	672	Operation on a Resource after Expiration or Release	1154	1488
HasMember	V	685	Function Call With Incorrect Number of Arguments	1154	1516
HasMember	V	686	Function Call With Incorrect Argument Type	1154	1517
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591
HasMember	B	771	Missing Reference to Active Allocated Resource	1154	1631
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1154	1632
HasMember	V	773	Missing Reference to Active File Descriptor or Handle	1154	1638
HasMember	V	775	Missing Release of File Descriptor or Handle after Effective Lifetime	1154	1640
HasMember	B	910	Use of Expired File Descriptor	1154	1809

References

[REF-607]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 09. Input Output (FIO)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152270 >.

[REF-987]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 09. Input Output (FIO)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151932 >.

Category-1165: SEI CERT C Coding Standard - Guidelines 10. Environment (ENV)

Category ID : 1165

Summary

Weaknesses in this category are related to the rules and recommendations in the Environment (ENV) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1154	155
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1154	198
HasMember	B	676	Use of Potentially Dangerous Function	1154	1498
HasMember	C	705	Incorrect Control Flow Scoping	1154	1550

References

[REF-608]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 10. Environment (ENV)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152421 >.

[REF-988]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec. 10. Environment (ENV)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151968 >.

Category-1166: SEI CERT C Coding Standard - Guidelines 11. Signals (SIG)

Category ID : 1166

Summary

Weaknesses in this category are related to the rules and recommendations in the Signals (SIG) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	V	479	Signal Handler Use of a Non-reentrant Function	1154	1154
HasMember	C	662	Improper Synchronization	1154	1457

References

[REF-609]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 11. Signals (SIG)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152469 >.

[REF-989]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 11. Signals (SIG)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151975 >.

Category-1167: SEI CERT C Coding Standard - Guidelines 12. Error Handling (ERR)

Category ID : 1167

Summary

Weaknesses in this category are related to the rules and recommendations in the Error Handling (ERR) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	252	Unchecked Return Value	1154	613
HasMember	B	253	Incorrect Check of Function Return Value	1154	620
HasMember	B	391	Unchecked Error Condition	1154	955
HasMember	V	456	Missing Initialization of a Variable	1154	1096
HasMember	B	676	Use of Potentially Dangerous Function	1154	1498
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591

References

[REF-610]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 12. Error Handling (ERR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152345 >.

[REF-990]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 12. Error Handling (ERR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151977 >.

Category-1168: SEI CERT C Coding Standard - Guidelines 13. Application Programming Interfaces (API)

Category ID : 1168

Summary

Weaknesses in this category are related to the rules and recommendations in the Application Programming Interfaces (API) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604

References

[REF-611]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 13. Application Programming Interfaces (API)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152242 >.

[REF-991]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 13. Application Programming Interfaces (API)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151980 >.

Category-1169: SEI CERT C Coding Standard - Guidelines 14. Concurrency (CON)

Category ID : 1169

Summary

Weaknesses in this category are related to the rules and recommendations in the Concurrency (CON) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	C	330	Use of Insufficiently Random Values	1154	821
HasMember	B	366	Race Condition within a Thread	1154	910
HasMember	C	377	Insecure Temporary File	1154	932
HasMember	C	667	Improper Locking	1154	1472
HasMember	B	676	Use of Potentially Dangerous Function	1154	1498

References

[REF-612]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 14. Concurrency (CON)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152257 >.

[REF-992]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 14. Concurrency (CON)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151970 >.

Category-1170: SEI CERT C Coding Standard - Guidelines 48. Miscellaneous (MSC)

Category ID : 1170

Summary

Weaknesses in this category are related to the rules and recommendations in the Miscellaneous (MSC) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1154	806
HasMember	C	330	Use of Insufficiently Random Values	1154	821
HasMember	B	331	Insufficient Entropy	1154	828
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	1154	844
HasMember	B	676	Use of Potentially Dangerous Function	1154	1498
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1154	1591

References

[REF-613]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 48. Miscellaneous (MSC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152201 >.

[REF-993]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 48. Miscellaneous (MSC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151973 >.

Category-1171: SEI CERT C Coding Standard - Guidelines 50. POSIX (POS)

Category ID : 1171

Summary

Weaknesses in this category are related to the rules and recommendations in the POSIX (POS) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	B	170	Improper Null Termination	1154	434
HasMember	B	242	Use of Inherently Dangerous Function	1154	593
HasMember	B	252	Unchecked Return Value	1154	613
HasMember	B	253	Incorrect Check of Function Return Value	1154	620
HasMember	B	273	Improper Check for Dropped Privileges	1154	667
HasMember	B	363	Race Condition Enabling Link Following	1154	904
HasMember	B	391	Unchecked Error Condition	1154	955
HasMember	C	667	Improper Locking	1154	1472
HasMember	C	696	Incorrect Behavior Order	1154	1535

References

[REF-614]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 50. POSIX (POS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87152405 >.

[REF-994]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 50. POSIX (POS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151931 >.

Category-1172: SEI CERT C Coding Standard - Guidelines 51. Microsoft Windows (WIN)

Category ID : 1172

Summary

Weaknesses in this category are related to the rules and recommendations in the Microsoft Windows (WIN) section of the SEI CERT C Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1154	Weaknesses Addressed by the SEI CERT C Coding Standard	1154	2604
HasMember	V	590	Free of Memory not on the Heap	1154	1335
HasMember	V	762	Mismatched Memory Management Routines	1154	1605

References

[REF-617]The Software Engineering Institute. "SEI CERT C Coding Standard : Rule 51. Microsoft Windows (WIN)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151925 >.

[REF-995]The Software Engineering Institute. "SEI CERT C Coding Standard : Rec 51. Microsoft Windows (WIN)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=87151933 >.

Category-1175: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 18. Concurrency (CON)

Category ID : 1175

Summary

Weaknesses in this category are related to the rules and recommendations in the Concurrency (CON) section of the SEI CERT Oracle Secure Coding Standard for Java.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1133	Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java	1133	2603

References

[REF-1007]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java : Rec 18. Concurrency (CON)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88487352 >.

Category-1179: SEI CERT Perl Coding Standard - Guidelines 01. Input Validation and Data Sanitization (IDS)

Category ID : 1179

Summary

Weaknesses in this category are related to the rules and recommendations in the Input Validation and Data Sanitization (IDS) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1178	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1178	148
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	1178	232
HasMember	C	116	Improper Encoding or Escaping of Output	1178	287
HasMember	V	129	Improper Validation of Array Index	1178	347
HasMember	B	134	Use of Externally-Controlled Format String	1178	371
HasMember	V	789	Memory Allocation with Excessive Size Value	1178	1683

References

[REF-1012]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 01. Input Validation and Data Sanitization (IDS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890533 >.

[REF-1020]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 01. Input Validation and Data Sanitization (IDS)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890568 >.

Category-1180: SEI CERT Perl Coding Standard - Guidelines 02. Declarations and Initialization (DCL)

Category ID : 1180

Summary

Weaknesses in this category are related to the rules and recommendations in the Declarations and Initialization (DCL) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	V	456	Missing Initialization of a Variable	1178	1096
HasMember	V	457	Use of Uninitialized Variable	1178	1102
HasMember	B	477	Use of Obsolete Function	1178	1146
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1178	1407

References

[REF-1013]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 02. Declarations and Initialization (DCL)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890509 >.

[REF-1021]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 02. Declarations and Initialization (DCL)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890569 >.

Category-1181: SEI CERT Perl Coding Standard - Guidelines 03. Expressions (EXP)

Category ID : 1181

Summary

Weaknesses in this category are related to the rules and recommendations in the Expressions (EXP) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	B	248	Uncaught Exception	1178	603
HasMember	B	252	Unchecked Return Value	1178	613
HasMember	B	375	Returning a Mutable Object to an Untrusted Caller	1178	930
HasMember	B	391	Unchecked Error Condition	1178	955
HasMember	B	394	Unexpected Status Code or Return Value	1178	962
HasMember	B	460	Improper Cleanup on Thrown Exception	1178	1109
HasMember	B	477	Use of Obsolete Function	1178	1146
HasMember	V	597	Use of Wrong Operator in String Comparison	1178	1345
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1178	1407
HasMember	∞	690	Unchecked Return Value to NULL Pointer Dereference	1178	1523
HasMember	C	705	Incorrect Control Flow Scoping	1178	1550
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1178	1577
HasMember	B	783	Operator Precedence Logic Error	1178	1659

References

[REF-1014]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 03. Expressions (EXP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890504 >.

[REF-1022]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 03. Expressions (EXP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890559 >.

Category-1182: SEI CERT Perl Coding Standard - Guidelines 04. Integers (INT)

Category ID : 1182

Summary

Weaknesses in this category are related to the rules and recommendations in the Integers (INT) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	C	189	Numeric Errors	1178	2333

References

[REF-1015]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 04. Integers (INT)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890508 >.

[REF-1023]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 04. Integers (INT)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890560 >.

Category-1183: SEI CERT Perl Coding Standard - Guidelines 05. Strings (STR)

Category ID : 1183

Summary

Weaknesses in this category are related to the rules and recommendations in the Strings (STR) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606

References

[REF-1016]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 05. Strings (STR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890507 >.

[REF-1024]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 05. Strings (STR)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890563 >.

Category-1184: SEI CERT Perl Coding Standard - Guidelines 06. Object-Oriented Programming (OOP)

Category ID : 1184

Summary

Weaknesses in this category are related to the rules and recommendations in the Object-Oriented Programming (OOP) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	B	767	Access to Critical Private Variable via Public Method	1178	1619

References

[REF-1017]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 06. Object-Oriented Programming (OOP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890501 >.

[REF-1025]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 06. Object-Oriented Programming (OOP)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890561 >.

Category-1185: SEI CERT Perl Coding Standard - Guidelines 07. File Input and Output (FIO)

Category ID : 1185

Summary

Weaknesses in this category are related to the rules and recommendations in the File Input and Output (FIO) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	1178	112

References

[REF-1018]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 07. File Input and Output (FIO)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890499 >.

[REF-1026]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rec. 07. File Input and Output (FIO)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890496 >.

Category-1186: SEI CERT Perl Coding Standard - Guidelines 50. Miscellaneous (MSC)

Category ID : 1186

Summary

Weaknesses in this category are related to the rules and recommendations in the Miscellaneous (MSC) section of the SEI CERT Perl Coding Standard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1178	Weaknesses Addressed by the SEI CERT Perl Coding Standard	1178	2606
HasMember	B	561	Dead Code	1178	1283
HasMember	B	563	Assignment to Variable without Use	1178	1289

References

[REF-1019]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 50. Miscellaneous (MSC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890497 >.

[REF-1027]The Software Engineering Institute. "SEI CERT Perl Coding Standard : Rule 50. Miscellaneous (MSC)". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88890502 >.

Category-1195: Manufacturing and Life Cycle Management Concerns

Category ID : 1195

Summary

Weaknesses in this category are root-caused to defects that arise in the semiconductor-manufacturing process or during the life cycle and supply chain.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	C	1059	Insufficient Technical Documentation	1194	1904
HasMember	B	1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications	1194	2060
HasMember	B	1266	Improper Scrubbing of Sensitive Data from Decommissioned Device	1194	2104
HasMember	B	1269	Product Released in Non-Release Configuration	1194	2110
HasMember	B	1273	Device Unlock Credential Sharing	1194	2119
HasMember	B	1297	Unprotected Confidential Information on Device is Accessible by OSAT Vendors	1194	2168

Category-1196: Security Flow Issues

Category ID : 1196

Summary

Weaknesses in this category are related to improper design of full-system security flows, including but not limited to secure boot, secure update, and hardware-device attestation.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1190	DMA Device Enabled Too Early in Boot Phase	1194	1987
HasMember	B	1193	Power-On of Untrusted Execution Core Before Enabling Fabric Access Control	1194	1995
HasMember	B	1264	Hardware Logic with Insecure De-Synchronization between Control and Data Channels	1194	2098
HasMember	B	1274	Improper Access Control for Volatile Memory Containing Boot Code	1194	2121
HasMember	B	1283	Mutable Attestation or Measurement Reporting Data	1194	2140
HasMember	B	1310	Missing Ability to Patch ROM Code	1194	2191
HasMember	B	1326	Missing Immutable Root of Trust in Hardware	1194	2224
HasMember	B	1328	Security Version Number Mutable to Older Versions	1194	2229

Category-1197: Integration Issues

Category ID : 1197

Summary

Weaknesses in this category are those that arise due to integration of multiple hardware Intellectual Property (IP) cores, from System-on-a-Chip (SoC) subsystem interactions, or from hardware platform subsystem interactions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1276	Hardware Child Block Incorrectly Connected to Parent System	1194	2125

Category-1198: Privilege Separation and Access Control Issues

Category ID : 1198

Summary

Weaknesses in this category are related to features and mechanisms providing hardware-based isolation and access control (e.g., identity, policy, locking control) of sensitive shared hardware resources such as registers and fuses.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
MemberOf	C	1372	ICS Supply Chain: OT Counterfeit and Malicious Corruption	1358	2530
HasMember	B	276	Incorrect Default Permissions	1194	672
HasMember	C	441	Unintended Proxy or Intermediary ('Confused Deputy')	1194	1072
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1194	1985
HasMember	B	1192	Improper Identifier for IP Block used in System-On-Chip (SOC)	1194	1994
HasMember	B	1220	Insufficient Granularity of Access Control	1194	2002
HasMember	V	1222	Insufficient Granularity of Address Regions Protected by Register Locks	1194	2010
HasMember	B	1242	Inclusion of Undocumented Features or Chicken Bits	1194	2044
HasMember	B	1260	Improper Handling of Overlap Between Protected Memory Ranges	1194	2087
HasMember	B	1262	Improper Access Control for Register Interface	1194	2093
HasMember	B	1267	Policy Uses Obsolete Encoding	1194	2105
HasMember	B	1268	Policy Privileges are not Assigned Consistently Between Control and Data Agents	1194	2107
HasMember	B	1280	Access Control Check Implemented After Asset is Accessed	1194	2134
HasMember	C	1294	Insecure Security Identifier Mechanism	1194	2162
HasMember	B	1299	Missing Protection Mechanism for Alternate Hardware Interface	1194	2174
HasMember	B	1302	Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC)	1194	2185

Nature	Type	ID	Name	V	Page
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1194	2186
HasMember	B	1314	Missing Write Protection for Parametric Data Values	1194	2199
HasMember	B	1318	Missing Support for Security Features in On-chip Fabrics or Buses	1194	2209
HasMember	B	1334	Unauthorized Error Injection Can Degrade Hardware Redundancy	1194	2246
HasMember	B	1420	Exposure of Sensitive Information during Transient Execution	1194	2297

Category-1199: General Circuit and Logic Design Concerns

Category ID : 1199

Summary

Weaknesses in this category are related to hardware-circuit design and logic (e.g., CMOS transistors, finite state machines, and registers) as well as issues related to hardware description languages such as System Verilog and VHDL.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1209	Failure to Disable Reserved Bits	1194	2000
HasMember	B	1221	Incorrect Register Defaults or Module Parameters	1194	2005
HasMember	B	1223	Race Condition for Write-Once Attributes	1194	2011
HasMember	B	1224	Improper Restriction of Write-Once Bit Fields	1194	2014
HasMember	B	1231	Improper Prevention of Lock Bit Modification	1194	2018
HasMember	B	1232	Improper Lock Behavior After Power State Transition	1194	2021
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	1194	2023
HasMember	B	1234	Hardware Internal or Debug Modes Allow Override of Locks	1194	2026
HasMember	B	1245	Improper Finite State Machines (FSMs) in Hardware Logic	1194	2052
HasMember	B	1250	Improper Preservation of Consistency Between Independent Representations of Shared State	1194	2064
HasMember	B	1253	Incorrect Selection of Fuse Values	1194	2069
HasMember	B	1254	Incorrect Comparison Logic Granularity	1194	2071
HasMember	B	1261	Improper Handling of Single Event Upsets	1194	2091
HasMember	B	1298	Hardware Logic Contains Race Conditions	1194	2170

Category-1201: Core and Compute Issues

Category ID : 1201

Summary

Weaknesses in this category are typically associated with CPUs, Graphics, Vision, AI, FPGA, and microcontrollers.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1252	CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations	1194	2068
HasMember	B	1281	Sequence of Processor Instructions Leads to Unexpected Behavior	1194	2136
HasMember	B	1342	Information Exposure through Microarchitectural State after Transient Execution	1194	2262
HasMember	B	1420	Exposure of Sensitive Information during Transient Execution	1194	2297

Category-1202: Memory and Storage Issues

Category ID : 1202

Summary

Weaknesses in this category are typically associated with memory (e.g., DRAM, SRAM) and storage technologies (e.g., NAND Flash, OTP, EEPROM, and eMMC).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	226	Sensitive Information in Resource Not Removed Before Reuse	1194	569
HasMember	B	1246	Improper Write Handling in Limited-write Non-Volatile Memories	1194	2054
HasMember	B	1251	Mirrored Regions with Different Values	1194	2065
HasMember	B	1257	Improper Access Control Applied to Mirrored or Aliased Memory Regions	1194	2079
HasMember	B	1282	Assumed-Immutable Data is Stored in Writable Memory	1194	2139
HasMember	B	1420	Exposure of Sensitive Information during Transient Execution	1194	2297

Category-1203: Peripherals, On-chip Fabric, and Interface/IO Problems

Category ID : 1203

Summary

Weaknesses in this category are related to hardware security problems that apply to peripheral devices, IO interfaces, on-chip interconnects, network-on-chip (NoC), and buses. For example, this category includes issues related to design of hardware interconnect and/or protocols such as PCIe, USB, SMBUS, general-purpose IO pins, and user-input peripherals such as mouse and keyboard.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1311	Improper Translation of Security Attributes by Fabric Bridge	1194	2194

Nature	Type	ID	Name	V	Page
HasMember	B	1312	Missing Protection for Mirrored Regions in On-Chip Fabric Firewall	1194	2196
HasMember	B	1315	Improper Setting of Bus Controlling Capability in Fabric End-point	1194	2202
HasMember	B	1316	Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges	1194	2204
HasMember	B	1317	Improper Access Control in Fabric Bridge	1194	2206
HasMember	B	1331	Improper Isolation of Shared Resources in Network On Chip (NoC)	1194	2237

Category-1205: Security Primitives and Cryptography Issues

Category ID : 1205

Summary

Weaknesses in this category are related to hardware implementations of cryptographic protocols and other hardware-security primitives such as physical unclonable functions (PUFs) and random number generators (RNGs).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	203	Observable Discrepancy	1194	525
HasMember	B	325	Missing Cryptographic Step	1194	801
HasMember	B	1240	Use of a Cryptographic Primitive with a Risky Implementation	1194	2036
HasMember	B	1241	Use of Predictable Algorithm in Random Number Generator	1194	2042
HasMember	B	1279	Cryptographic Operations are run Before Supporting Units are Ready	1194	2132
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1194	2265

Category-1206: Power, Clock, Thermal, and Reset Concerns

Category ID : 1206

Summary

Weaknesses in this category are related to system power, voltage, current, temperature, clocks, system state saving/restoring, and resets at the platform and SoC level.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1232	Improper Lock Behavior After Power State Transition	1194	2021
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1194	2056
HasMember	B	1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications	1194	2060

Nature	Type	ID	Name	V	Page
HasMember	V	1255	Comparison Logic is Vulnerable to Power Side-Channel Attacks	1194	2073
HasMember	B	1256	Improper Restriction of Software Interfaces to Hardware Features	1194	2076
HasMember	B	1271	Uninitialized Value on Reset for Registers Holding Security Settings	1194	2115
HasMember	B	1304	Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation	1194	2188
HasMember	B	1314	Missing Write Protection for Parametric Data Values	1194	2199
HasMember	B	1320	Improper Protection for Outbound Error Messages and Alert Signals	1194	2214
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1194	2240
HasMember	B	1338	Improper Protections Against Hardware Overheating	1194	2252

Category-1207: Debug and Test Problems

Category ID : 1207

Summary

Weaknesses in this category are related to hardware debug and test interfaces such as JTAG and scan chain.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	319	Cleartext Transmission of Sensitive Information	1194	786
HasMember	B	1191	On-Chip Debug and Test Interface With Improper Access Control	1194	1989
HasMember	B	1234	Hardware Internal or Debug Modes Allow Override of Locks	1194	2026
HasMember	B	1243	Sensitive Non-Volatile Information Not Protected During Debug	1194	2046
HasMember	B	1244	Internal Asset Exposed to Unsafe Debug Access Level or State	1194	2048
HasMember	B	1258	Exposure of Sensitive System Information Due to Uncleared Debug Information	1194	2082
HasMember	B	1272	Sensitive Information Uncleared Before Debug/Power State Transition	1194	2116
HasMember	B	1291	Public Key Re-Use for Signing both Debug and Production Code	1194	2157
HasMember	B	1295	Debug Messages Revealing Unnecessary Information	1194	2164
HasMember	B	1296	Incorrect Chaining or Granularity of Debug Components	1194	2166
HasMember	B	1313	Hardware Allows Activation of Test or Debug Logic at Runtime	1194	2198
HasMember	B	1323	Improper Management of Sensitive Trace Data	1194	2220

Category-1208: Cross-Cutting Problems

Category ID : 1208

Summary

Weaknesses in this category can arise in multiple areas of hardware design or can apply to a wide cross-section of components.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	440	Expected Behavior Violation	1194	1069
HasMember	B	1053	Missing Documentation for Design	1194	1898
HasMember	C	1059	Insufficient Technical Documentation	1194	1904
HasMember	C	1263	Improper Physical Access Control	1194	2097
HasMember	B	1277	Firmware Not Updateable	1194	2128
HasMember	B	1301	Insufficient or Incomplete Data Removal within Hardware Component	1194	2183
HasMember	B	1329	Reliance on Component That is Not Updateable	1194	2231
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1194	2266

Category-1210: Audit / Logging Errors

Category ID : 1210

Summary

Weaknesses in this category are related to audit-based components of a software system. Frequently these deal with logging user activities in order to identify undesired access and modifications to the system. The weaknesses in this category could lead to a degradation of the quality of the audit capability if they are not addressed.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	117	Improper Output Neutralization for Logs	699	294
HasMember	B	222	Truncation of Security-relevant Information	699	565
HasMember	B	223	Omission of Security-relevant Information	699	566
HasMember	B	224	Obscured Security-relevant Information by Alternate Name	699	568
HasMember	B	778	Insufficient Logging	699	1647
HasMember	B	779	Logging of Excessive Data	699	1651

Category-1211: Authentication Errors

Category ID : 1211

Summary

Weaknesses in this category are related to authentication components of a system. Frequently these deal with the ability to verify that an entity is indeed who it claims to be. If not addressed when designing or implementing a software system, these weaknesses could lead to a degradation of the quality of the authentication capability.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	289	Authentication Bypass by Alternate Name	699	710
HasMember	B	290	Authentication Bypass by Spoofing	699	712
HasMember	B	294	Authentication Bypass by Capture-replay	699	719
HasMember	B	295	Improper Certificate Validation	699	721
HasMember	B	301	Reflection Attack in an Authentication Protocol	699	740
HasMember	B	303	Incorrect Implementation of Authentication Algorithm	699	744
HasMember	B	305	Authentication Bypass by Primary Weakness	699	747
HasMember	B	306	Missing Authentication for Critical Function	699	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	699	754
HasMember	B	308	Use of Single-factor Authentication	699	759
HasMember	B	309	Use of Password System for Primary Authentication	699	761
HasMember	B	322	Key Exchange without Entity Authentication	699	795
HasMember	B	603	Use of Client-Side Authentication	699	1363
HasMember	B	645	Overly Restrictive Account Lockout Mechanism	699	1432
HasMember	B	804	Guessable CAPTCHA	699	1710
HasMember	B	836	Use of Password Hash Instead of Password for Authentication	699	1770

Category-1212: Authorization Errors

Category ID : 1212

Summary

Weaknesses in this category are related to authorization components of a system. Frequently these deal with the ability to enforce that agents have the required permissions before performing certain operations, such as modifying data. If not addressed when designing or implementing a software system, these weaknesses could lead to a degradation of the quality of the authorization capability.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	425	Direct Request ('Forced Browsing')	699	1032
HasMember	B	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	699	1273
HasMember	B	552	Files or Directories Accessible to External Parties	699	1274
HasMember	B	639	Authorization Bypass Through User-Controlled Key	699	1415
HasMember	C	653	Improper Isolation or Compartmentalization	699	1445
HasMember	B	842	Placement of User into Incorrect Group	699	1784
HasMember	B	939	Improper Authorization in Handler for Custom URL Scheme	699	1849
HasMember	B	1220	Insufficient Granularity of Access Control	699	2002
HasMember	B	1230	Exposure of Sensitive Information Through Metadata	699	2017

Category-1213: Random Number Issues

Category ID : 1213

Summary

Weaknesses in this category are related to a software system's random number generation.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	331	Insufficient Entropy	699	828
HasMember	B	334	Small Space of Random Values	699	834
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	699	836
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	699	844
HasMember	B	341	Predictable from Observable State	699	850
HasMember	B	342	Predictable Exact Value from Previous Values	699	852
HasMember	B	343	Predictable Value Range from Previous Values	699	854
HasMember	B	344	Use of Invariant Value in Dynamically Changing Context	699	856
HasMember	B	1241	Use of Predictable Algorithm in Random Number Generator	699	2042

Category-1214: Data Integrity Issues

Category ID : 1214

Summary

Weaknesses in this category are related to a software system's data integrity components. Frequently these deal with the ability to ensure the integrity of data, such as messages, resource files, deployment files, and configuration files. The weaknesses in this category could lead to a degradation of data integrity quality if they are not addressed.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	322	Key Exchange without Entity Authentication	699	795
HasMember	C	346	Origin Validation Error	699	860
HasMember	B	347	Improper Verification of Cryptographic Signature	699	864
HasMember	B	348	Use of Less Trusted Source	699	866
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	699	868
HasMember	B	351	Insufficient Type Distinction	699	873
HasMember	B	353	Missing Support for Integrity Check	699	881
HasMember	B	354	Improper Validation of Integrity Check Value	699	883
HasMember	B	494	Download of Code Without Integrity Check	699	1192
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	699	1292
HasMember	B	649	Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking	699	1439
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	699	1750

Nature	Type	ID	Name	V	Page
HasMember	B	924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel	699	1839

Category-1215: Data Validation Issues

Category ID : 1215

Summary

Weaknesses in this category are related to a software system's components for input validation, output validation, or other kinds of validation. Validation is a frequently-used technique for ensuring that data conforms to expectations before it is further processed as input or output. There are many varieties of validation (see CWE-20, which is just for input validation). Validation is distinct from other techniques that attempt to modify data before processing it, although developers may consider all attempts to product "safe" inputs or outputs as some kind of validation. Regardless, validation is a powerful tool that is often used to minimize malformed data from entering the system, or indirectly avoid code injection or other potentially-malicious patterns when generating output. The weaknesses in this category could lead to a degradation of the quality of data flow in a system if they are not addressed.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	112	Missing XML Validation	699	275
HasMember	B	179	Incorrect Behavior Order: Early Validation	699	454
HasMember	B	183	Permissive List of Allowed Inputs	699	464
HasMember	B	184	Incomplete List of Disallowed Inputs	699	466
HasMember	B	606	Unchecked Input for Loop Condition	699	1366
HasMember	B	641	Improper Restriction of Names for Files and Other Resources	699	1421
HasMember	B	1173	Improper Use of Validation Framework	699	1978
HasMember	B	1284	Improper Validation of Specified Quantity in Input	699	2142
HasMember	B	1285	Improper Validation of Specified Index, Position, or Offset in Input	699	2144
HasMember	B	1286	Improper Validation of Syntactic Correctness of Input	699	2148
HasMember	B	1287	Improper Validation of Specified Type of Input	699	2150
HasMember	B	1288	Improper Validation of Consistency within Input	699	2151
HasMember	B	1289	Improper Validation of Unsafe Equivalence in Input	699	2153

Notes

Relationship

CWE-20 (Improper Input Validation) is not included in this category because it is a Class level, and this category focuses more on Base level weaknesses. Also note that other kinds of weaknesses besides improper validation are included as members of this category.

Category-1216: Lockout Mechanism Errors

Category ID : 1216

Summary

Weaknesses in this category are related to a software system's lockout mechanism. Frequently these deal with scenarios that take effect in case of multiple failed attempts to access a given resource. The weaknesses in this category could lead to a degradation of access to system assets if they are not addressed.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
MemberOf	C	1353	OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures	1344	2515
HasMember	B	645	Overly Restrictive Account Lockout Mechanism	699	1432

Category-1217: User Session Errors

Category ID : 1217

Summary

Weaknesses in this category are related to session management. Frequently these deal with the information or status about each user and their access rights for the duration of multiple requests. The weaknesses in this category could lead to a degradation of the quality of session management if they are not addressed.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	488	Exposure of Data Element to Wrong Session	699	1176
HasMember	B	613	Insufficient Session Expiration	699	1380
HasMember	B	841	Improper Enforcement of Behavioral Workflow	699	1781

Category-1218: Memory Buffer Errors

Category ID : 1218

Summary

Weaknesses in this category are related to the handling of memory buffers within a software system.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	699	310
HasMember	B	124	Buffer Underwrite ('Buffer Underflow')	699	332
HasMember	B	125	Out-of-bounds Read	699	336
HasMember	B	131	Incorrect Calculation of Buffer Size	699	361
HasMember	B	786	Access of Memory Location Before Start of Buffer	699	1666
HasMember	B	787	Out-of-bounds Write	699	1669
HasMember	B	788	Access of Memory Location After End of Buffer	699	1678
HasMember	B	805	Buffer Access with Incorrect Length Value	699	1711

Nature	Type	ID	Name	V	Page
HasMember	B	1284	Improper Validation of Specified Quantity in Input	699	2142

Category-1219: File Handling Issues

Category ID : 1219

Summary

Weaknesses in this category are related to the handling of files within a software system. Files, directories, and folders are so central to information technology that many different weaknesses and variants have been discovered.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	699	33
HasMember	B	41	Improper Resolution of Path Equivalence	699	87
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	699	112
HasMember	B	66	Improper Handling of File Names that Identify Virtual Resources	699	125
HasMember	B	378	Creation of Temporary File With Insecure Permissions	699	935
HasMember	B	379	Creation of Temporary File in Directory with Insecure Permissions	699	937
HasMember	B	426	Untrusted Search Path	699	1035
HasMember	B	427	Uncontrolled Search Path Element	699	1040
HasMember	B	428	Unquoted Search Path or Element	699	1047

Category-1225: Documentation Issues

Category ID : 1225

Summary

Weaknesses in this category are related to the documentation provided to support, create, or analyze a product.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	1053	Missing Documentation for Design	699	1898
HasMember	B	1068	Inconsistency Between Implementation and Documented Design	699	1915
HasMember	B	1110	Incomplete Design Documentation	699	1959
HasMember	B	1111	Incomplete I/O Documentation	699	1960
HasMember	B	1112	Incomplete Documentation of Program Execution	699	1961
HasMember	B	1118	Insufficient Documentation of Error Handling Techniques	699	1967

Category-1226: Complexity Issues

Category ID : 1226

Summary

Weaknesses in this category are associated with things being overly complex.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	1043	Data Element Aggregating an Excessively Large Number of Non-Primitive Elements	699	1887
HasMember	B	1047	Modules with Circular Dependencies	699	1891
HasMember	B	1055	Multiple Inheritance from Concrete Classes	699	1900
HasMember	B	1056	Invokable Control Element with Variadic Parameters	699	1901
HasMember	B	1060	Excessive Number of Inefficient Server-Side Data Accesses	699	1906
HasMember	B	1064	Invokable Control Element with Signature Containing an Excessive Number of Parameters	699	1911
HasMember	B	1074	Class with Excessively Deep Inheritance	699	1923
HasMember	B	1075	Unconditional Control Flow Transfer outside of Switch Block	699	1924
HasMember	B	1080	Source Code File with Excessive Number of Lines of Code	699	1930
HasMember	B	1086	Class with Excessive Number of Child Classes	699	1935
HasMember	B	1095	Loop Condition Value Update within the Loop	699	1944
HasMember	B	1119	Excessive Use of Unconditional Branching	699	1968
HasMember	B	1121	Excessive McCabe Cyclomatic Complexity	699	1970
HasMember	B	1122	Excessive Halstead Complexity	699	1971
HasMember	B	1123	Excessive Use of Self-Modifying Code	699	1972
HasMember	B	1124	Excessively Deep Nesting	699	1973
HasMember	B	1125	Excessive Attack Surface	699	1974
HasMember	B	1333	Inefficient Regular Expression Complexity	699	2243

Category-1227: Encapsulation Issues

Category ID : 1227

Summary

Weaknesses in this category are related to issues surrounding the bundling of data with the methods intended to operate on that data.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer	699	1899
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component	699	1902
HasMember	B	1062	Parent Class with References to Child Class	699	1909

Nature	Type	ID	Name	V	Page
HasMember	B	1083	Data Access from Outside Expected Data Manager Component	699	1932
HasMember	B	1090	Method Containing Access of a Member Element from Another Class	699	1939
HasMember	B	1100	Insufficient Isolation of System-Dependent Functions	699	1949
HasMember	B	1105	Insufficient Encapsulation of Machine-Dependent Functionality	699	1954

Category-1228: API / Function Errors

Category ID : 1228

Summary

Weaknesses in this category are related to the use of built-in functions or external APIs.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	699	Software Development	699	2576
HasMember	B	242	Use of Inherently Dangerous Function	699	593
HasMember	B	474	Use of Function with Inconsistent Implementations	699	1136
HasMember	B	475	Undefined Behavior for Input to API	699	1138
HasMember	B	477	Use of Obsolete Function	699	1146
HasMember	B	676	Use of Potentially Dangerous Function	699	1498
HasMember	B	695	Use of Low-Level Functionality	699	1533
HasMember	B	749	Exposed Dangerous Method or Function	699	1572

Category-1237: SFP Primary Cluster: Faulty Resource Release

Category ID : 1237

Summary

This category identifies Software Fault Patterns (SFPs) within the Faulty Resource Release cluster (SFP37).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	V	415	Double Free	888	1015
HasMember	V	762	Mismatched Memory Management Routines	888	1605
HasMember	B	763	Release of Invalid Pointer or Reference	888	1608

Category-1238: SFP Primary Cluster: Failure to Release Memory

Category ID : 1238

Summary

This category identifies Software Fault Patterns (SFPs) within the Failure to Release Memory cluster (SFP38).

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	888	Software Fault Pattern (SFP) Clusters	888	2592
HasMember	V	401	Missing Release of Memory after Effective Lifetime	888	980

Category-1306: CISQ Quality Measures - Reliability

Category ID : 1306

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Reliability. Presence of these weaknesses could reduce the reliability of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1305	CISQ Quality Measures (2020)	1305	2609
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1305	299
HasMember	B	170	Improper Null Termination	1305	434
HasMember	B	252	Unchecked Return Value	1305	613
HasMember	B	390	Detection of Error Condition Without Action	1305	950
HasMember	B	394	Unexpected Status Code or Return Value	1305	962
HasMember	C	404	Improper Resource Shutdown or Release	1305	987
HasMember	C	424	Improper Protection of Alternate Path	1305	1031
HasMember	B	459	Incomplete Cleanup	1305	1106
HasMember	B	476	NULL Pointer Dereference	1305	1139
HasMember	B	480	Use of Incorrect Operator	1305	1157
HasMember	B	484	Omitted Break Statement in Switch	1305	1169
HasMember	B	562	Return of Stack Variable Address	1305	1287
HasMember	V	595	Comparison of Object References Instead of Object Contents	1305	1342
HasMember	C	662	Improper Synchronization	1305	1457
HasMember	C	665	Improper Initialization	1305	1465
HasMember	C	672	Operation on a Resource after Expiration or Release	1305	1488
HasMember	B	681	Incorrect Conversion between Numeric Types	1305	1504
HasMember	P	682	Incorrect Calculation	1305	1507
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1305	1544
HasMember	C	704	Incorrect Type Conversion or Cast	1305	1547
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1305	1591
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1305	1766
HasMember	B	908	Use of Uninitialized Resource	1305	1802
HasMember	B	1045	Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor	1305	1889
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1305	1896
HasMember	B	1066	Missing Serialization Control Element	1305	1913

Nature	Type	ID	Name	V	Page
HasMember	B	1070	Serializable Data Element Containing non-Serializable Item Elements	1305	1918
HasMember	V	1077	Floating Point Comparison with Incorrect Operator	1305	1926
HasMember	B	1079	Parent Class without Virtual Destructor Method	1305	1929
HasMember	B	1082	Class Instance Self Destruction Control Element	1305	1931
HasMember	B	1083	Data Access from Outside Expected Data Manager Component	1305	1932
HasMember	B	1087	Class with Virtual Method without a Virtual Destructor	1305	1936
HasMember	B	1088	Synchronous Access of Remote Resource without Timeout	1305	1937
HasMember	B	1098	Data Element containing Pointer Item without Proper Copy Control Element	1305	1947

References

[REF-1133]Consortium for Information & Software Quality (CISQ). "Automated Source Code Quality Measures". 2020. < https://www.omg.org/spec/ASCQM/ >.

Category-1307: CISQ Quality Measures - Maintainability

Category ID : 1307

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Maintainability. Presence of these weaknesses could reduce the maintainability of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1305	CISQ Quality Measures (2020)	1305	2609
HasMember	C	407	Inefficient Algorithmic Complexity	1305	999
HasMember	B	478	Missing Default Case in Multiple Condition Expression	1305	1149
HasMember	B	480	Use of Incorrect Operator	1305	1157
HasMember	B	484	Omitted Break Statement in Switch	1305	1169
HasMember	B	561	Dead Code	1305	1283
HasMember	B	570	Expression is Always False	1305	1300
HasMember	B	571	Expression is Always True	1305	1303
HasMember	B	783	Operator Precedence Logic Error	1305	1659
HasMember	B	1041	Use of Redundant Code	1305	1884
HasMember	B	1045	Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor	1305	1889
HasMember	B	1047	Modules with Circular Dependencies	1305	1891
HasMember	B	1048	Invokable Control Element with Large Number of Outward Calls	1305	1892
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1305	1896
HasMember	B	1052	Excessive Use of Hard-Coded Literals in Initialization	1305	1897
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer	1305	1899
HasMember	B	1055	Multiple Inheritance from Concrete Classes	1305	1900
HasMember	B	1062	Parent Class with References to Child Class	1305	1909

Nature	Type	ID	Name	V	Page
HasMember	B	1064	Invokable Control Element with Signature Containing an Excessive Number of Parameters	1305	1911
HasMember	B	1074	Class with Excessively Deep Inheritance	1305	1923
HasMember	B	1075	Unconditional Control Flow Transfer outside of Switch Block	1305	1924
HasMember	B	1079	Parent Class without Virtual Destructor Method	1305	1929
HasMember	B	1080	Source Code File with Excessive Number of Lines of Code	1305	1930
HasMember	B	1084	Invokable Control Element with Excessive File or Data Access Operations	1305	1933
HasMember	B	1085	Invokable Control Element with Excessive Volume of Commented-out Code	1305	1934
HasMember	B	1086	Class with Excessive Number of Child Classes	1305	1935
HasMember	B	1087	Class with Virtual Method without a Virtual Destructor	1305	1936
HasMember	B	1090	Method Containing Access of a Member Element from Another Class	1305	1939
HasMember	B	1095	Loop Condition Value Update within the Loop	1305	1944

References

[REF-1133]Consortium for Information & Software Quality (CISQ). "Automated Source Code Quality Measures". 2020. < https://www.omg.org/spec/ASCQM/ >.

Category-1308: CISQ Quality Measures - Security

Category ID : 1308

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Security. Presence of these weaknesses could reduce the security of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1305	CISQ Quality Measures (2020)	1305	2609
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1305	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1305	148
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1305	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1305	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	1305	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	1305	220
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	1305	249
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1305	299
HasMember	V	129	Improper Validation of Array Index	1305	347
HasMember	B	134	Use of Externally-Controlled Format String	1305	371
HasMember	B	252	Unchecked Return Value	1305	613

Nature	Type	ID	Name	V	Page
HasMember	C	404	Improper Resource Shutdown or Release	1305	987
HasMember	C	424	Improper Protection of Alternate Path	1305	1031
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1305	1055
HasMember	B	477	Use of Obsolete Function	1305	1146
HasMember	B	480	Use of Incorrect Operator	1305	1157
HasMember	B	502	Deserialization of Untrusted Data	1305	1212
HasMember	B	570	Expression is Always False	1305	1300
HasMember	B	571	Expression is Always True	1305	1303
HasMember	B	606	Unchecked Input for Loop Condition	1305	1366
HasMember	B	611	Improper Restriction of XML External Entity Reference	1305	1376
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1305	1428
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1305	1444
HasMember	C	662	Improper Synchronization	1305	1457
HasMember	C	665	Improper Initialization	1305	1465
HasMember	C	672	Operation on a Resource after Expiration or Release	1305	1488
HasMember	B	681	Incorrect Conversion between Numeric Types	1305	1504
HasMember	P	682	Incorrect Calculation	1305	1507
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1305	1559
HasMember	B	778	Insufficient Logging	1305	1647
HasMember	B	783	Operator Precedence Logic Error	1305	1659
HasMember	V	789	Memory Allocation with Excessive Size Value	1305	1683
HasMember	B	798	Use of Hard-coded Credentials	1305	1699
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1305	1766

References

[REF-1133]Consortium for Information & Software Quality (CISQ). "Automated Source Code Quality Measures". 2020. < https://www.omg.org/spec/ASCQM/ >.

Category-1309: CISQ Quality Measures - Efficiency

Category ID : 1309

Summary

Weaknesses in this category are related to the CISQ Quality Measures for Efficiency. Presence of these weaknesses could reduce the efficiency of the software.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1305	CISQ Quality Measures (2020)	1305	2609
HasMember	C	404	Improper Resource Shutdown or Release	1305	987
HasMember	C	424	Improper Protection of Alternate Path	1305	1031
HasMember	V	1042	Static Member Data Element outside of a Singleton Class Element	1305	1886
HasMember	B	1043	Data Element Aggregating an Excessively Large Number of Non-Primitive Elements	1305	1887
HasMember	B	1046	Creation of Immutable Text Using String Concatenation	1305	1890

Nature	Type	ID	Name	V	Page
HasMember	B	1049	Excessive Data Query Operations in a Large Data Table	1305	1894
HasMember	B	1050	Excessive Platform Resource Consumption within a Loop	1305	1895
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component	1305	1902
HasMember	B	1060	Excessive Number of Inefficient Server-Side Data Accesses	1305	1906
HasMember	B	1067	Excessive Execution of Sequential Searches of Data Resource	1305	1914
HasMember	B	1072	Data Resource Access without Use of Connection Pooling	1305	1921
HasMember	B	1073	Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses	1305	1922
HasMember	B	1089	Large Data Table with Excessive Number of Indices	1305	1938
HasMember	B	1091	Use of Object without Invoking Destructor Method	1305	1940
HasMember	B	1094	Excessive Index Range Scan for a Data Resource	1305	1943

References

[REF-1133]Consortium for Information & Software Quality (CISQ). "Automated Source Code Quality Measures". 2020. < https://www.omg.org/spec/ASCQM/ >.

Category-1345: OWASP Top Ten 2021 Category A01:2021 - Broken Access Control

Category ID : 1345

Summary

Weaknesses in this category are related to the A01 category "Broken Access Control" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1344	33
HasMember	B	23	Relative Path Traversal	1344	46
HasMember	V	35	Path Traversal: '.../...//'	1344	73
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	1344	112
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	1344	511
HasMember	B	201	Insertion of Sensitive Information Into Sent Data	1344	521
HasMember	V	219	Storage of File with Sensitive Data Under Web Root	1344	560
HasMember	C	264	Permissions, Privileges, and Access Controls	1344	2337
HasMember	C	275	Permission Issues	1344	2339
HasMember	B	276	Incorrect Default Permissions	1344	672
HasMember	P	284	Improper Access Control	1344	687
HasMember	C	285	Improper Authorization	1344	691
HasMember	B	352	Cross-Site Request Forgery (CSRF)	1344	875

Nature	Type	ID	Name	V	Page
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	1344	889
HasMember	C	377	Insecure Temporary File	1344	932
HasMember	C	402	Transmission of Private Resources into a New Sphere ('Resource Leak')	1344	984
HasMember	B	425	Direct Request ('Forced Browsing')	1344	1032
HasMember	C	441	Unintended Proxy or Intermediary ('Confused Deputy')	1344	1072
HasMember	B	497	Exposure of Sensitive System Information to an Unauthorized Control Sphere	1344	1201
HasMember	B	538	Insertion of Sensitive Information into Externally-Accessible File or Directory	1344	1257
HasMember	B	540	Inclusion of Sensitive Information in Source Code	1344	1260
HasMember	V	548	Exposure of Information Through Directory Listing	1344	1269
HasMember	B	552	Files or Directories Accessible to External Parties	1344	1274
HasMember	V	566	Authorization Bypass Through User-Controlled SQL Primary Key	1344	1294
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1344	1353
HasMember	B	639	Authorization Bypass Through User-Controlled Key	1344	1415
HasMember	V	651	Exposure of WSDL File Containing Sensitive Information	1344	1442
HasMember	C	668	Exposure of Resource to Wrong Sphere	1344	1478
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	1344	1553
HasMember	C	862	Missing Authorization	1344	1789
HasMember	C	863	Incorrect Authorization	1344	1796
HasMember	C	913	Improper Control of Dynamically-Managed Code Resources	1344	1814
HasMember	C	922	Insecure Storage of Sensitive Information	1344	1835
HasMember	V	1275	Sensitive Cookie with Improper SameSite Attribute	1344	2123

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories, which are discouraged for mapping, as well as high-level weaknesses such as Pillars. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1207]"A01:2021 - Broken Access Control". 2021 September 4. OWASP. < https://owasp.org/Top10/A01_2021-Broken_Access_Control/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1346: OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures

Category ID : 1346

Summary

Weaknesses in this category are related to the A02 category "Cryptographic Failures" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	B	261	Weak Encoding for Password	1344	638
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	1344	726
HasMember	C	310	Cryptographic Issues	1344	2339
HasMember	B	319	Cleartext Transmission of Sensitive Information	1344	786
HasMember	V	321	Use of Hard-coded Cryptographic Key	1344	792
HasMember	B	322	Key Exchange without Entity Authentication	1344	795
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	1344	797
HasMember	B	324	Use of a Key Past its Expiration Date	1344	799
HasMember	B	325	Missing Cryptographic Step	1344	801
HasMember	C	326	Inadequate Encryption Strength	1344	803
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1344	806
HasMember	B	328	Use of Weak Hash	1344	813
HasMember	V	329	Generation of Predictable IV with CBC Mode	1344	818
HasMember	C	330	Use of Insufficiently Random Values	1344	821
HasMember	B	331	Insufficient Entropy	1344	828
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	1344	836
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1344	839
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1344	841
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	1344	844
HasMember	C	340	Generation of Predictable Numbers or Identifiers	1344	849
HasMember	B	347	Improper Verification of Cryptographic Signature	1344	864
HasMember	B	523	Unprotected Transport of Credentials	1344	1239
HasMember	C	720	OWASP Top Ten 2007 Category A9 - Insecure Communications	1344	2354
HasMember	B	757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')	1344	1589
HasMember	V	759	Use of a One-Way Hash without a Salt	1344	1593
HasMember	V	760	Use of a One-Way Hash with a Predictable Salt	1344	1598
HasMember	V	780	Use of RSA Algorithm without OAEP	1344	1652
HasMember	C	818	OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection	1344	2381
HasMember	B	916	Use of Password Hash With Insufficient Computational Effort	1344	1822

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories, which are discouraged for mapping, as well as high-level weaknesses such as Pillars. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1208]"A02:2021 - Cryptographic Failures". 2021 September 4. OWASP. < https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1347: OWASP Top Ten 2021 Category A03:2021 - Injection

Category ID : 1347

Summary

Weaknesses in this category are related to the A03 category "Injection" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	C	20	Improper Input Validation	1344	20
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1344	138
HasMember	C	75	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)	1344	145
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1344	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1344	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1344	168
HasMember	V	80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	1344	182
HasMember	V	83	Improper Neutralization of Script in Attributes in a Web Page	1344	188
HasMember	V	87	Improper Neutralization of Alternate XSS Syntax	1344	196
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1344	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1344	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	1344	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	1344	220
HasMember	B	93	Improper Neutralization of CRLF Sequences ('CRLF Injection')	1344	222
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	1344	225
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	1344	232
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	1344	238
HasMember	V	97	Improper Neutralization of Server-Side Includes (SSI) Within a Web Page	1344	241
HasMember	V	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	1344	242
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	1344	249

Nature	Type	ID	Name	V	Page
HasMember	V	113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')	1344	277
HasMember	C	116	Improper Encoding or Escaping of Output	1344	287
HasMember	C	138	Improper Neutralization of Special Elements	1344	379
HasMember	B	184	Incomplete List of Disallowed Inputs	1344	466
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1344	1125
HasMember	B	471	Modification of Assumed-Immutable Data (MAID)	1344	1129
HasMember	V	564	SQL Injection: Hibernate	1344	1290
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1344	1373
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1344	1428
HasMember	V	644	Improper Neutralization of HTTP Headers for Scripting Syntax	1344	1430
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1344	1444
HasMember	B	917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	1344	1827

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include high-level Class and/or Pillar weaknesses. The CWE Program will work with OWASP to improve these mappings, possibly including modifications to CWE itself.

References

[REF-1209]"A03:2021 - Injection". 2021 September 4. OWASP. < https://owasp.org/Top10/A03_2021-Injection/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1348: OWASP Top Ten 2021 Category A04:2021 - Insecure Design

Category ID : 1348

Summary

Weaknesses in this category are related to the A04 "Insecure Design" category in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	B	73	External Control of File Name or Path	1344	133
HasMember	B	183	Permissive List of Allowed Inputs	1344	464
HasMember	B	209	Generation of Error Message Containing Sensitive Information	1344	540
HasMember	B	213	Exposure of Sensitive Information Due to Incompatible Policies	1344	555

Nature	Type	ID	Name	V	Page
HasMember	V	235	Improper Handling of Extra Parameters	1344	585
HasMember	B	256	Plaintext Storage of a Password	1344	622
HasMember	B	257	Storing Passwords in a Recoverable Format	1344	625
HasMember	B	266	Incorrect Privilege Assignment	1344	645
HasMember	C	269	Improper Privilege Management	1344	653
HasMember	B	280	Improper Handling of Insufficient Permissions or Privileges	1344	679
HasMember	C	311	Missing Encryption of Sensitive Data	1344	764
HasMember	B	312	Cleartext Storage of Sensitive Information	1344	771
HasMember	V	313	Cleartext Storage in a File or on Disk	1344	777
HasMember	V	316	Cleartext Storage of Sensitive Information in Memory	1344	782
HasMember	B	419	Unprotected Primary Channel	1344	1024
HasMember	B	430	Deployment of Wrong Handler	1344	1049
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1344	1055
HasMember	B	444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	1344	1075
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1344	1087
HasMember	B	472	External Control of Assumed-Immutable Web Parameter	1344	1131
HasMember	B	501	Trust Boundary Violation	1344	1210
HasMember	C	522	Insufficiently Protected Credentials	1344	1234
HasMember	V	525	Use of Web Browser Cache Containing Sensitive Information	1344	1242
HasMember	V	539	Use of Persistent Cookies Containing Sensitive Information	1344	1259
HasMember	V	579	J2EE Bad Practices: Non-serializable Object Stored in Session	1344	1318
HasMember	V	598	Use of GET Request Method With Sensitive Query Strings	1344	1349
HasMember	C	602	Client-Side Enforcement of Server-Side Security	1344	1359
HasMember	C	642	External Control of Critical State Data	1344	1422
HasMember	V	646	Reliance on File Name or Extension of Externally-Supplied File	1344	1434
HasMember	V	650	Trusting HTTP Permission Methods on the Server Side	1344	1441
HasMember	C	653	Improper Isolation or Compartmentalization	1344	1445
HasMember	C	656	Reliance on Security Through Obscurity	1344	1452
HasMember	C	657	Violation of Secure Design Principles	1344	1454
HasMember	C	799	Improper Control of Interaction Frequency	1344	1708
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1344	1723
HasMember	C	840	Business Logic Errors	1344	2381
HasMember	B	841	Improper Enforcement of Behavioral Workflow	1344	1781
HasMember	V	927	Use of Implicit Intent for Sensitive Communication	1344	1846
HasMember	B	1021	Improper Restriction of Rendered UI Layers or Frames	1344	1869
HasMember	B	1173	Improper Use of Validation Framework	1344	1978

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories, which are discouraged

for mapping, as well as high-level weaknesses such as Pillars. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1210]"A04:2021 - Insecure Design". 2021 September 4. OWASP. < https://owasp.org/Top10/A04_2021-Insecure_Design/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1349: OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration

Category ID : 1349

Summary

Weaknesses in this category are related to the A05 category "Security Misconfiguration" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	C	2	7PK - Environment	1344	2329
HasMember	V	11	ASP.NET Misconfiguration: Creating Debug Binary	1344	9
HasMember	V	13	ASP.NET Misconfiguration: Password in Configuration File	1344	13
HasMember	B	15	External Control of System or Configuration Setting	1344	17
HasMember	C	16	Configuration	1344	2330
HasMember	B	260	Password in Configuration File	1344	636
HasMember	V	315	Cleartext Storage of Sensitive Information in a Cookie	1344	781
HasMember	V	520	.NET Misconfiguration: Use of Impersonation	1344	1230
HasMember	V	526	Cleartext Storage of Sensitive Information in an Environment Variable	1344	1243
HasMember	V	537	Java Runtime Error Message Containing Sensitive Information	1344	1255
HasMember	V	541	Inclusion of Sensitive Information in an Include File	1344	1262
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	1344	1267
HasMember	B	611	Improper Restriction of XML External Entity Reference	1344	1376
HasMember	V	614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	1344	1382
HasMember	B	756	Missing Custom Error Page	1344	1588
HasMember	B	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	1344	1642
HasMember	V	942	Permissive Cross-domain Policy with Untrusted Domains	1344	1857
HasMember	V	1004	Sensitive Cookie Without 'HttpOnly' Flag	1344	1863
HasMember	C	1032	OWASP Top Ten 2017 Category A6 - Security Misconfiguration	1344	2459
HasMember	V	1174	ASP.NET Misconfiguration: Improper Model Validation	1344	1979

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories, which are discouraged for mapping. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1211]"A05:2021 - Security Misconfiguration". 2021 September 4. OWASP. < https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1352: OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components

Category ID : 1352

Summary

Weaknesses in this category are related to the A06 category "Vulnerable and Outdated Components" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	C	937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities	1344	2413
HasMember	C	1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities	1344	2460
HasMember	B	1104	Use of Unmaintained Third Party Components	1344	1953

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories, which are discouraged for mapping. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1212]"A06:2021 - Vulnerable and Outdated Components". 2021 September 4. OWASP. < https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1353: OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures

Category ID : 1353

Summary

Weaknesses in this category are related to the A07 category "Identification and Authentication Failures" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	C	255	Credentials Management Errors	1344	2336
HasMember	V	259	Use of Hard-coded Password	1344	630
HasMember	C	287	Improper Authentication	1344	699
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1344	707
HasMember	B	290	Authentication Bypass by Spoofing	1344	712
HasMember	B	294	Authentication Bypass by Capture-replay	1344	719
HasMember	B	295	Improper Certificate Validation	1344	721
HasMember	V	297	Improper Validation of Certificate with Host Mismatch	1344	729
HasMember	C	300	Channel Accessible by Non-Endpoint	1344	737
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	1344	742
HasMember	B	304	Missing Critical Step in Authentication	1344	745
HasMember	B	306	Missing Authentication for Critical Function	1344	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	1344	754
HasMember	C	346	Origin Validation Error	1344	860
HasMember	B	384	Session Fixation	1344	943
HasMember	B	521	Weak Password Requirements	1344	1231
HasMember	B	613	Insufficient Session Expiration	1344	1380
HasMember	B	620	Unverified Password Change	1344	1392
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	1344	1418
HasMember	B	798	Use of Hard-coded Credentials	1344	1699
HasMember	B	940	Improper Verification of Source of a Communication Channel	1344	1852
HasMember	C	1216	Lockout Mechanism Errors	1344	2499

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories, which are discouraged for mapping, as well as high-level weaknesses. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1213]"A07:2021 - Identification and Authentication Failures". 2021 September 4. OWASP. < https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1354: OWASP Top Ten 2021 Category A08:2021 - Software and Data Integrity Failures

Category ID : 1354

Summary

Weaknesses in this category are related to the A08 category "Software and Data Integrity Failures" in the OWASP Top Ten 2021.

Membership

2516

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	C	345	Insufficient Verification of Data Authenticity	1344	858
HasMember	B	353	Missing Support for Integrity Check	1344	881
HasMember	B	426	Untrusted Search Path	1344	1035
HasMember	B	494	Download of Code Without Integrity Check	1344	1192
HasMember	B	502	Deserialization of Untrusted Data	1344	1212
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	1344	1292
HasMember	V	784	Reliance on Cookies without Validation and Integrity Checking in a Security Decision	1344	1662
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1344	1750
HasMember	V	830	Inclusion of Web Functionality from an Untrusted Source	1344	1756
HasMember	B	915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	1344	1818

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1214]"A08:2021 - Software and Data Integrity Failures". 2021 September 4. OWASP. < https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1355: OWASP Top Ten 2021 Category A09:2021 - Security Logging and Monitoring Failures

Category ID : 1355

Summary

Weaknesses in this category are related to the A09 category "Security Logging and Monitoring Failures" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	B	117	Improper Output Neutralization for Logs	1344	294
HasMember	B	223	Omission of Security-relevant Information	1344	566
HasMember	B	532	Insertion of Sensitive Information into Log File	1344	1250
HasMember	B	778	Insufficient Logging	1344	1647

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1215]"A09:2021 - Security Logging and Monitoring Failures". 2021 September 4. OWASP. < https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1356: OWASP Top Ten 2021 Category A10:2021 - Server-Side Request Forgery (SSRF)

Category ID : 1356

Summary

Weaknesses in this category are related to the A10 category "Server-Side Request Forgery (SSRF)" in the OWASP Top Ten 2021.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2614
HasMember	B	918	Server-Side Request Forgery (SSRF)	1344	1829

Notes

Maintenance

As of CWE 4.6, the relationships in this category were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1216]"A10:2021 - Server-Side Request Forgery (SSRF)". 2021 September 4. OWASP. < https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/ >.

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Category-1359: ICS Communications

Category ID : 1359

Summary

Weaknesses in this category are related to the "ICS Communications" super category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1358	Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS	1358	2617
HasMember	C	1364	ICS Communications: Zone Boundary Failures	1358	2522
HasMember	C	1365	ICS Communications: Unreliability	1358	2523
HasMember	C	1366	ICS Communications: Frail Security in Protocols	1358	2524

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1360: ICS Dependencies (& Architecture)

Category ID : 1360

Summary

Weaknesses in this category are related to the "ICS Dependencies (& Architecture)" super category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1358	Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS	1358	2617
HasMember	C	1367	ICS Dependencies (& Architecture): External Physical Systems	1358	2525
HasMember	C	1368	ICS Dependencies (& Architecture): External Digital Systems	1358	2526

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1361: ICS Supply Chain

Category ID : 1361

Summary

Weaknesses in this category are related to the "ICS Supply Chain" super category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1358	Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS	1358	2617
HasMember	C	1369	ICS Supply Chain: IT/OT Convergence/Expansion	1358	2527
HasMember	C	1370	ICS Supply Chain: Common Mode Frailties	1358	2528
HasMember	C	1371	ICS Supply Chain: Poorly Documented or Undocumented Features	1358	2529
HasMember	C	1372	ICS Supply Chain: OT Counterfeit and Malicious Corruption	1358	2530

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1362: ICS Engineering (Constructions/Deployment)

Category ID : 1362

Summary

Weaknesses in this category are related to the "ICS Engineering (Constructions/Deployment)" super category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1358	Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS	1358	2617
HasMember	C	1373	ICS Engineering (Construction/Deployment): Trust Model Problems	1358	2531

Nature	Type	ID	Name	V	Page
HasMember	C	1374	ICS Engineering (Construction/Deployment): Maker Breaker Blindness	1358	2531
HasMember	C	1375	ICS Engineering (Construction/Deployment): Gaps in Details/Data	1358	2532
HasMember	C	1376	ICS Engineering (Construction/Deployment): Security Gaps in Commissioning	1358	2533
HasMember	C	1377	ICS Engineering (Construction/Deployment): Inherent Predictability in Design	1358	2534

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1363: ICS Operations (& Maintenance)

Category ID : 1363

Summary

Weaknesses in this category are related to the "ICS Operations (& Maintenance)" super category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1358	Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS	1358	2617
HasMember	C	1378	ICS Operations (& Maintenance): Gaps in obligations and training	1358	2534
HasMember	C	1379	ICS Operations (& Maintenance): Human factors in ICS environments	1358	2535
HasMember	C	1380	ICS Operations (& Maintenance): Post-analysis changes	1358	2536
HasMember	C	1381	ICS Operations (& Maintenance): Exploitable Standard Operational Procedures	1358	2537
HasMember	C	1382	ICS Operations (& Maintenance): Emerging Energy Technologies	1358	2538
HasMember	C	1383	ICS Operations (& Maintenance): Compliance/ Conformance with Regulatory Requirements	1358	2538

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1364: ICS Communications: Zone Boundary Failures

Category ID : 1364

Summary

Weaknesses in this category are related to the "Zone Boundary Failures" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Within an ICS system, for traffic that crosses through network zone boundaries, vulnerabilities arise when those boundaries were designed for safety or other purposes but are being repurposed for security." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1359	ICS Communications	1358	2518
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	1358	551
HasMember	B	268	Privilege Chaining	1358	651
HasMember	C	269	Improper Privilege Management	1358	653
HasMember	C	287	Improper Authentication	1358	699
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1358	707
HasMember	B	306	Missing Authentication for Critical Function	1358	748
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	895
HasMember		384	Session Fixation	1358	943
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1358	1055
HasMember	B	494	Download of Code Without Integrity Check	1358	1192
HasMember	B	501	Trust Boundary Violation	1358	1210
HasMember	C	668	Exposure of Resource to Wrong Sphere	1358	1478
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1358	1480
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1358	1577

Nature	Type	ID	Name	V	Page
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1358	1750
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1358	1985
HasMember	C	1263	Improper Physical Access Control	1358	2097
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1358	2186
HasMember	B	1393	Use of Default Password	1358	2286

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1365: ICS Communications: Unreliability

Category ID : 1365

Summary

Weaknesses in this category are related to the "Unreliability" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Vulnerabilities arise in reaction to disruptions in the physical layer (e.g. creating electrical noise) used to carry the traffic." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1359	ICS Communications	1358	2518
HasMember	V	121	Stack-based Buffer Overflow	1358	320
HasMember	C	269	Improper Privilege Management	1358	653
HasMember	B	306	Missing Authentication for Critical Function	1358	748
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1358	868
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	895
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1358	1723
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1358	2056
HasMember	B	1261	Improper Handling of Single Event Upsets	1358	2091

Nature	Type	ID	Name	V	Page
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1358	2240
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1358	2265
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1358	2269

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1258]Wikipedia. "Random early detection". < https://en.wikipedia.org/wiki/Random_early_detection >.

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1366: ICS Communications: Frail Security in Protocols

Category ID : 1366

Summary

Weaknesses in this category are related to the "Frail Security in Protocols" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Vulnerabilities arise as a result of mis-implementation or incomplete implementation of security in ICS implementations of communication protocols." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1359	ICS Communications	1358	2518
HasMember	V	121	Stack-based Buffer Overflow	1358	320
HasMember	B	125	Out-of-bounds Read	1358	336
HasMember	B	268	Privilege Chaining	1358	651
HasMember	C	269	Improper Privilege Management	1358	653
HasMember	B	276	Incorrect Default Permissions	1358	672
HasMember	B	290	Authentication Bypass by Spoofing	1358	712
HasMember	B	306	Missing Authentication for Critical Function	1358	748
HasMember	C	311	Missing Encryption of Sensitive Data	1358	764
HasMember	B	312	Cleartext Storage of Sensitive Information	1358	771

Nature	Type	ID	Name	V	Page
HasMember	B	319	Cleartext Transmission of Sensitive Information	1358	786
HasMember	B	325	Missing Cryptographic Step	1358	801
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1358	806
HasMember	C	330	Use of Insufficiently Random Values	1358	821
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1358	839
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1358	841
HasMember	B	341	Predictable from Observable State	1358	850
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1358	868
HasMember	B	358	Improperly Implemented Security Check for Standard	1358	888
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	895
HasMember	C	377	Insecure Temporary File	1358	932
HasMember	F	384	Session Fixation	1358	943
HasMember	B	648	Incorrect Use of Privileged APIs	1358	1437
HasMember	B	787	Out-of-bounds Write	1358	1669
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1358	1985
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1358	2186
HasMember	B	1393	Use of Default Password	1358	2286

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1259]Wikipedia. "Transport Layer Security". < https://en.wikipedia.org/wiki/Transport_Layer_Security >.

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1367: ICS Dependencies (& Architecture): External Physical Systems

Category ID : 1367

Summary

Weaknesses in this category are related to the "External Physical Systems" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Due to the highly interconnected technologies in use, an external dependency on another physical system could cause an availability interruption for the protected system." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1360	ICS Dependencies (& Architecture)	1358	2519
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1358	2056
HasMember	B	1338	Improper Protections Against Hardware Overheating	1358	2252
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1358	2266
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1358	2269

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1368: ICS Dependencies (& Architecture): External Digital Systems

Category ID : 1368

Summary

Weaknesses in this category are related to the "External Digital Systems" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Due to the highly interconnected technologies in use, an external dependency on another digital system could cause a confidentiality, integrity, or availability incident for the protected system." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1360	ICS Dependencies (& Architecture)	1358	2519
HasMember	B	15	External Control of System or Configuration Setting	1358	17
HasMember	C	287	Improper Authentication	1358	699
HasMember	B	306	Missing Authentication for Critical Function	1358	748

Nature	Type	ID	Name	V	Page
HasMember	B	308	Use of Single-factor Authentication	1358	759
HasMember	B	312	Cleartext Storage of Sensitive Information	1358	771
HasMember	B	440	Expected Behavior Violation	1358	1069
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1358	1125
HasMember	B	603	Use of Client-Side Authentication	1358	1363
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1358	1373
HasMember	C	638	Not Using Complete Mediation	1358	1413
HasMember	C	1059	Insufficient Technical Documentation	1358	1904
HasMember	B	1068	Inconsistency Between Implementation and Documented Design	1358	1915
HasMember	B	1104	Use of Unmaintained Third Party Components	1358	1953
HasMember	B	1329	Reliance on Component That is Not Updateable	1358	2231
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1358	2266
HasMember	B	1393	Use of Default Password	1358	2286

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1369: ICS Supply Chain: IT/OT Convergence/Expansion

Category ID : 1369

Summary

Weaknesses in this category are related to the "IT/OT Convergence/Expansion" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "The increased penetration of DER devices and smart loads make emerging ICS networks more like IT networks and thus susceptible to vulnerabilities similar to those of IT networks." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1361	ICS Supply Chain	1358	2520
HasMember	P	284	Improper Access Control	1358	687

Nature	Type	ID	Name	V	Page
HasMember	C	636	Not Failing Securely ('Failing Open')	1358	1409

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.SITUATIONS (Focus on situations in which weaknesses may appear).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1370: ICS Supply Chain: Common Mode Frailties

Category ID : 1370

Summary

Weaknesses in this category are related to the "Common Mode Frailties" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "At the component level, most ICS systems are assembled from common parts made by other companies. One or more of these common parts might contain a vulnerability that could result in a wide-spread incident." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1361	ICS Supply Chain	1358	2520
HasMember	V	329	Generation of Predictable IV with CBC Mode	1358	818
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1358	1463
HasMember	P	693	Protection Mechanism Failure	1358	1529
HasMember	P	707	Improper Neutralization	1358	1554
HasMember	P	710	Improper Adherence to Coding Standards	1358	1558
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1358	2266

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1260]Thu T. Pham. "The Great DNS Vulnerability of 2008 by Dan Kaminsky". 2016 April 6. < https://duo.com/blog/the-great-dns-vulnerability-of-2008-by-dan-kaminsky >.

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1371: ICS Supply Chain: Poorly Documented or Undocumented Features

Category ID : 1371

Summary

Weaknesses in this category are related to the "Poorly Documented or Undocumented Features" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Undocumented capabilities and configurations pose a risk by not having a clear understanding of what the device is specifically supposed to do and only do. Therefore possibly opening up the attack surface and vulnerabilities." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1361	ICS Supply Chain	1358	2520
HasMember	B	489	Active Debug Code	1358	1178
HasMember	C	912	Hidden Functionality	1358	1812
HasMember	C	1059	Insufficient Technical Documentation	1358	1904
HasMember	B	1242	Inclusion of Undocumented Features or Chicken Bits	1358	2044

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1372: ICS Supply Chain: OT Counterfeit and Malicious Corruption

Category ID : 1372

Summary

Weaknesses in this category are related to the "OT Counterfeit and Malicious Corruption" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "In ICS, when this procurement process results in a vulnerability or component damage, it can have grid impacts or cause physical harm." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1361	ICS Supply Chain	1358	2520
HasMember	P	284	Improper Access Control	1358	687
HasMember	C	1198	Privilege Separation and Access Control Issues	1358	2491
HasMember	B	1231	Improper Prevention of Lock Bit Modification	1358	2018
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	1358	2023
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1358	2131

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1373: ICS Engineering (Construction/Deployment): Trust Model Problems

Category ID : 1373

Summary

Weaknesses in this category are related to the "Trust Model Problems" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Assumptions made about the user during the design or construction phase may result in vulnerabilities after the system is installed if the user operates it using a different security approach or process than what was designed or built." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1362	ICS Engineering (Constructions/Deployment)	1358	2520
HasMember	G	269	Improper Privilege Management	1358	653
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1358	868
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1358	1723

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1374: ICS Engineering (Construction/Deployment): Maker Breaker Blindness

Category ID : 1374

Summary

Weaknesses in this category are related to the "Maker Breaker Blindness" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Lack of awareness of deliberate attack techniques by people (vs failure modes from natural causes like weather or metal fatigue) may lead to insufficient security controls being built into ICS systems." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1362	ICS Engineering (Constructions/Deployment)	1358	2520

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1375: ICS Engineering (Construction/Deployment): Gaps in Details/Data

Category ID : 1375

Summary

Weaknesses in this category are related to the "Gaps in Details/Data" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Highly complex systems are often operated by personnel who have years of experience in managing that particular facility or plant. Much of their knowledge is passed along through verbal or hands-on training but may not be fully documented in written practices and procedures." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1362	ICS Engineering (Constructions/Deployment)	1358	2520
HasMember	P	710	Improper Adherence to Coding Standards	1358	1558
HasMember	B	1053	Missing Documentation for Design	1358	1898
HasMember	G	1059	Insufficient Technical Documentation	1358	1904
HasMember	B	1110	Incomplete Design Documentation	1358	1959
HasMember	B	1111	Incomplete I/O Documentation	1358	1960

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1376: ICS Engineering (Construction/Deployment): Security Gaps in Commissioning

Category ID : 1376

Summary

Weaknesses in this category are related to the "Security Gaps in Commissioning" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "As a large system is brought online components of the system may remain vulnerable until the entire system is operating and functional and security controls are put in place. This creates a window of opportunity for an adversary during the commissioning process." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1362	ICS Engineering (Constructions/Deployment)	1358	2520
HasMember	B	276	Incorrect Default Permissions	1358	672
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	895
HasMember	B	1393	Use of Default Password	1358	2286

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1377: ICS Engineering (Construction/Deployment): Inherent Predictability in Design

Category ID : 1377

Summary

Weaknesses in this category are related to the "Inherent Predictability in Design" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "The commonality of design (in ICS/SCADA architectures) for energy systems and environments opens up the possibility of scaled compromise by leveraging the inherent predictability in the design." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1362	ICS Engineering (Constructions/Deployment)	1358	2520
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1358	2131

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1378: ICS Operations (& Maintenance): Gaps in obligations and training

Category ID : 1378

Summary

Weaknesses in this category are related to the "Gaps in obligations and training" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "OT

ownership and responsibility for identifying and mitigating vulnerabilities are not clearly defined or communicated within an organization, leaving environments unpatched, exploitable, and with a broader attack surface." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1363	ICS Operations (& Maintenance)	1358	2521

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Subgroup members did not find any CWEs to add to this category in CWE 4.11. There may be some gaps with respect to CWE's current scope, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1261]Sam Weber, Paul A. Karger and Amit Paradkar. "A Software Flaw Taxonomy: Aiming Tools At Security". 2005. < https://cwe.mitre.org/documents/sources/ASoftwareFlawTaxonomy-AimingToolsatSecurity%5BWeber,Karger,Paradkar%5D.pdf >.2024-11-17.

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1379: ICS Operations (& Maintenance): Human factors in ICS environments

Category ID : 1379

Summary

Weaknesses in this category are related to the "Human factors in ICS environments" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Environmental factors in ICS including physical duress, system complexities, and isolation may result in security gaps or inadequacies in the performance of individual duties and responsibilities." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1363	ICS Operations (& Maintenance)	1358	2521

Nature	Type	ID	Name	V	Page
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1358	1087
HasMember	C	655	Insufficient Psychological Acceptability	1358	1450

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Subgroup members did not find any CWEs to add to this category in CWE 4.11. There may be some gaps with respect to CWE's current scope, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1380: ICS Operations (& Maintenance): Post-analysis changes

Category ID : 1380

Summary

Weaknesses in this category are related to the "Post-analysis changes" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Changes made to a previously analyzed and approved ICS environment can introduce new security vulnerabilities (as opposed to safety)." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1363	ICS Operations (& Maintenance)	1358	2521

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Subgroup members did not find any CWEs to add to this category in CWE 4.11. There may be some gaps with respect to CWE's current scope, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1381: ICS Operations (& Maintenance): Exploitable Standard Operational Procedures

Category ID : 1381

Summary

Weaknesses in this category are related to the "Exploitable Standard Operational Procedures" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "Standard ICS Operational Procedures developed for safety and operational functionality in a closed, controlled communications environment can introduce vulnerabilities in a more connected environment." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1363	ICS Operations (& Maintenance)	1358	2521

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This entry might be subject to CWE Scope Exclusions SCOPE.SITUATIONS (Focus on situations in which weaknesses may appear) and/or SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Subgroup members did not find any CWEs to add to this category in CWE 4.11. There may be some gaps with respect to CWE's current scope, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1382: ICS Operations (& Maintenance): Emerging Energy Technologies

Category ID : 1382

Summary

Weaknesses in this category are related to the "Emerging Energy Technologies" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "With the rapid evolution of the energy system accelerated by the emergence of new technologies such as DERs, electric vehicles, advanced communications (5G+), novel and diverse challenges arise for secure and resilient operation of the system." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1363	ICS Operations (& Maintenance)	1358	2521
HasMember	C	20	Improper Input Validation	1358	20
HasMember	C	285	Improper Authorization	1358	691
HasMember	B	295	Improper Certificate Validation	1358	721
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	1358	726
HasMember	C	346	Origin Validation Error	1358	860
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	1358	997
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1358	1353

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This category might be subject to CWE Scope Exclusion SCOPE.SITUATIONS (Focus on situations in which weaknesses may appear).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Subgroup members did not find any CWEs to add to this category in CWE 4.11. There may be some gaps with respect to CWE's current scope, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1383: ICS Operations (& Maintenance): Compliance/Conformance with Regulatory Requirements

Category ID : 1383

Summary

Weaknesses in this category are related to the "Compliance/Conformance with Regulatory Requirements" category from the SEI ETF "Categories of Security Vulnerabilities in ICS" as published in March 2022: "The ICS environment faces overlapping regulatory regimes and authorities with multiple focus areas (e.g., operational resiliency, physical safety, interoperability, and security) which can result in cyber security vulnerabilities when implemented as written due to gaps in considerations, outdatedness, or conflicting requirements." Note: members of this category include "Nearest IT Neighbor" recommendations from the report, as well as suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	C	1363	ICS Operations (& Maintenance)	1358	2521
HasMember	P	710	Improper Adherence to Coding Standards	1358	1558

Notes

Relationship

Relationships in this category are not authoritative and subject to change. See Maintenance notes.

Maintenance

This entry might be subject to CWE Scope Exclusions SCOPE.SITUATIONS (Focus on situations in which weaknesses may appear) and/or SCOPE.HUMANPROC (Human/organizational process).

Maintenance

This category was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Subgroup members did not find any CWEs to add to this category in CWE 4.11. There may be some gaps with respect to CWE's current scope, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Category-1388: Physical Access Issues and Concerns

Category ID : 1388

Summary

Weaknesses in this category are related to concerns of physical access.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1194	Hardware Design	1194	2607
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1194	2056
HasMember	B	1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications	1194	2060
HasMember	V	1255	Comparison Logic is Vulnerable to Power Side-Channel Attacks	1194	2073

Nature	Type	ID	Name	V	Page
HasMember	B	1261	Improper Handling of Single Event Upsets	1194	2091
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1194	2131
HasMember	B	1300	Improper Protection of Physical Side Channels	1194	2177
HasMember	B	1319	Improper Protection against Electromagnetic Fault Injection (EM-FI)	1194	2212
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1194	2240
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1194	2265
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1194	2269

Category-1396: Comprehensive Categorization: Access Control

Category ID : 1396

Summary

Weaknesses in this category are related to access control.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	9	J2EE Misconfiguration: Weak Access Permissions for EJB Methods	1400	8
HasMember	V	13	ASP.NET Misconfiguration: Password in Configuration File	1400	13
HasMember	B	202	Exposure of Sensitive Information Through Data Queries	1400	523
HasMember	B	256	Plaintext Storage of a Password	1400	622
HasMember	B	257	Storing Passwords in a Recoverable Format	1400	625
HasMember	V	258	Empty Password in Configuration File	1400	628
HasMember	V	259	Use of Hard-coded Password	1400	630
HasMember	B	260	Password in Configuration File	1400	636
HasMember	B	261	Weak Encoding for Password	1400	638
HasMember	B	262	Not Using Password Aging	1400	640
HasMember	B	263	Password Aging with Long Expiration	1400	643
HasMember	B	266	Incorrect Privilege Assignment	1400	645
HasMember	B	267	Privilege Defined With Unsafe Actions	1400	648
HasMember	B	268	Privilege Chaining	1400	651
HasMember	C	269	Improper Privilege Management	1400	653
HasMember	B	270	Privilege Context Switching Error	1400	659
HasMember	C	271	Privilege Dropping / Lowering Errors	1400	660
HasMember	B	272	Least Privilege Violation	1400	663
HasMember	B	273	Improper Check for Dropped Privileges	1400	667
HasMember	B	274	Improper Handling of Insufficient Privileges	1400	670
HasMember	B	276	Incorrect Default Permissions	1400	672
HasMember	V	277	Insecure Inherited Permissions	1400	675

Nature	Type	ID	Name	V	Page
HasMember	V	278	Insecure Preserved Inherited Permissions	1400	676
HasMember	V	279	Incorrect Execution-Assigned Permissions	1400	678
HasMember	B	280	Improper Handling of Insufficient Permissions or Privileges	1400	679
HasMember	B	281	Improper Preservation of Permissions	1400	681
HasMember	C	282	Improper Ownership Management	1400	683
HasMember	B	283	Unverified Ownership	1400	685
HasMember	P	284	Improper Access Control	1400	687
HasMember	C	285	Improper Authorization	1400	691
HasMember	C	286	Incorrect User Management	1400	698
HasMember	C	287	Improper Authentication	1400	699
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1400	707
HasMember	B	289	Authentication Bypass by Alternate Name	1400	710
HasMember	B	290	Authentication Bypass by Spoofing	1400	712
HasMember	V	291	Reliance on IP Address for Authentication	1400	715
HasMember	V	293	Using Referer Field for Authentication	1400	717
HasMember	B	294	Authentication Bypass by Capture-replay	1400	719
HasMember	B	295	Improper Certificate Validation	1400	721
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	1400	726
HasMember	V	297	Improper Validation of Certificate with Host Mismatch	1400	729
HasMember	V	298	Improper Validation of Certificate Expiration	1400	733
HasMember	B	299	Improper Check for Certificate Revocation	1400	734
HasMember	C	300	Channel Accessible by Non-Endpoint	1400	737
HasMember	B	301	Reflection Attack in an Authentication Protocol	1400	740
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	1400	742
HasMember	B	303	Incorrect Implementation of Authentication Algorithm	1400	744
HasMember	B	304	Missing Critical Step in Authentication	1400	745
HasMember	B	305	Authentication Bypass by Primary Weakness	1400	747
HasMember	B	306	Missing Authentication for Critical Function	1400	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	1400	754
HasMember	B	308	Use of Single-factor Authentication	1400	759
HasMember	B	309	Use of Password System for Primary Authentication	1400	761
HasMember	V	321	Use of Hard-coded Cryptographic Key	1400	792
HasMember	B	322	Key Exchange without Entity Authentication	1400	795
HasMember	V	350	Reliance on Reverse DNS Resolution for a Security-Critical Action	1400	870
HasMember	V	370	Missing Check for Certificate Revocation after Initial Check	1400	924
HasMember		384	Session Fixation	1400	943
HasMember	B	419	Unprotected Primary Channel	1400	1024
HasMember	B	420	Unprotected Alternate Channel	1400	1025
HasMember	B	421	Race Condition During Access to Alternate Channel	1400	1028
HasMember	V	422	Unprotected Windows Messaging Channel ('Shatter')	1400	1029
HasMember	B	425	Direct Request ('Forced Browsing')	1400	1032
HasMember	C	441	Unintended Proxy or Intermediary ('Confused Deputy')	1400	1072
HasMember	V	520	.NET Misconfiguration: Use of Impersonation	1400	1230
HasMember	B	521	Weak Password Requirements	1400	1231

Nature	Type	ID	Name	V	Page
HasMember	C	522	Insufficiently Protected Credentials	1400	1234
HasMember	B	523	Unprotected Transport of Credentials	1400	1239
HasMember	B	549	Missing Password Field Masking	1400	1271
HasMember	B	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	1400	1273
HasMember	V	555	J2EE Misconfiguration: Plaintext Password in Configuration File	1400	1279
HasMember	V	556	ASP.NET Misconfiguration: Use of Identity Impersonation	1400	1280
HasMember	V	566	Authorization Bypass Through User-Controlled SQL Primary Key	1400	1294
HasMember	V	593	Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created	1400	1339
HasMember	V	599	Missing Validation of OpenSSL Certificate	1400	1350
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1400	1353
HasMember	B	603	Use of Client-Side Authentication	1400	1363
HasMember	B	611	Improper Restriction of XML External Entity Reference	1400	1376
HasMember	B	612	Improper Authorization of Index Containing Sensitive Information	1400	1379
HasMember	B	613	Insufficient Session Expiration	1400	1380
HasMember	B	620	Unverified Password Change	1400	1392
HasMember	V	623	Unsafe ActiveX Control Marked Safe For Scripting	1400	1397
HasMember	B	639	Authorization Bypass Through User-Controlled Key	1400	1415
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	1400	1418
HasMember	B	645	Overly Restrictive Account Lockout Mechanism	1400	1432
HasMember	V	647	Use of Non-Canonical URL Paths for Authorization Decisions	1400	1435
HasMember	B	648	Incorrect Use of Privileged APIs	1400	1437
HasMember	B	708	Incorrect Ownership Assignment	1400	1556
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1400	1559
HasMember	B	798	Use of Hard-coded Credentials	1400	1699
HasMember	B	804	Guessable CAPTCHA	1400	1710
HasMember	B	836	Use of Password Hash Instead of Password for Authentication	1400	1770
HasMember	B	842	Placement of User into Incorrect Group	1400	1784
HasMember	C	862	Missing Authorization	1400	1789
HasMember	C	863	Incorrect Authorization	1400	1796
HasMember	B	918	Server-Side Request Forgery (SSRF)	1400	1829
HasMember	B	921	Storage of Sensitive Data in a Mechanism without Access Control	1400	1834
HasMember	C	923	Improper Restriction of Communication Channel to Intended Endpoints	1400	1836
HasMember	V	925	Improper Verification of Intent by Broadcast Receiver	1400	1841
HasMember	V	926	Improper Export of Android Application Components	1400	1843
HasMember	V	927	Use of Implicit Intent for Sensitive Communication	1400	1846
HasMember	B	939	Improper Authorization in Handler for Custom URL Scheme	1400	1849
HasMember	B	940	Improper Verification of Source of a Communication Channel	1400	1852

Nature	Type	ID	Name	V	Page
HasMember	B	941	Incorrectly Specified Destination in a Communication Channel	1400	1855
HasMember	V	942	Permissive Cross-domain Policy with Untrusted Domains	1400	1857
HasMember	V	1004	Sensitive Cookie Without 'HttpOnly' Flag	1400	1863
HasMember	B	1021	Improper Restriction of Rendered UI Layers or Frames	1400	1869
HasMember	V	1022	Use of Web Link to Untrusted Target with window.opener Access	1400	1872
HasMember	B	1191	On-Chip Debug and Test Interface With Improper Access Control	1400	1989
HasMember	B	1220	Insufficient Granularity of Access Control	1400	2002
HasMember	V	1222	Insufficient Granularity of Address Regions Protected by Register Locks	1400	2010
HasMember	B	1224	Improper Restriction of Write-Once Bit Fields	1400	2014
HasMember	B	1230	Exposure of Sensitive Information Through Metadata	1400	2017
HasMember	B	1231	Improper Prevention of Lock Bit Modification	1400	2018
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	1400	2023
HasMember	B	1242	Inclusion of Undocumented Features or Chicken Bits	1400	2044
HasMember	B	1243	Sensitive Non-Volatile Information Not Protected During Debug	1400	2046
HasMember	B	1244	Internal Asset Exposed to Unsafe Debug Access Level or State	1400	2048
HasMember	B	1252	CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations	1400	2068
HasMember	B	1256	Improper Restriction of Software Interfaces to Hardware Features	1400	2076
HasMember	B	1257	Improper Access Control Applied to Mirrored or Aliased Memory Regions	1400	2079
HasMember	B	1259	Improper Restriction of Security Token Assignment	1400	2085
HasMember	B	1260	Improper Handling of Overlap Between Protected Memory Ranges	1400	2087
HasMember	B	1262	Improper Access Control for Register Interface	1400	2093
HasMember	C	1263	Improper Physical Access Control	1400	2097
HasMember	B	1267	Policy Uses Obsolete Encoding	1400	2105
HasMember	B	1268	Policy Privileges are not Assigned Consistently Between Control and Data Agents	1400	2107
HasMember	B	1270	Generation of Incorrect Security Tokens	1400	2113
HasMember	B	1274	Improper Access Control for Volatile Memory Containing Boot Code	1400	2121
HasMember	V	1275	Sensitive Cookie with Improper SameSite Attribute	1400	2123
HasMember	B	1276	Hardware Child Block Incorrectly Connected to Parent System	1400	2125
HasMember	B	1283	Mutable Attestation or Measurement Reporting Data	1400	2140
HasMember	B	1290	Incorrect Decoding of Security Identifiers	1400	2155
HasMember	B	1292	Incorrect Conversion of Security Identifiers	1400	2159
HasMember	C	1294	Insecure Security Identifier Mechanism	1400	2162
HasMember	B	1296	Incorrect Chaining or Granularity of Debug Components	1400	2166
HasMember	B	1297	Unprotected Confidential Information on Device is Accessible by OSAT Vendors	1400	2168

Nature	Type	ID	Name	V	Page
HasMember	B	1299	Missing Protection Mechanism for Alternate Hardware Interface	1400	2174
HasMember	B	1302	Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC)	1400	2185
HasMember	B	1304	Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation	1400	2188
HasMember	B	1311	Improper Translation of Security Attributes by Fabric Bridge	1400	2194
HasMember	B	1312	Missing Protection for Mirrored Regions in On-Chip Fabric Firewall	1400	2196
HasMember	B	1313	Hardware Allows Activation of Test or Debug Logic at Runtime	1400	2198
HasMember	B	1314	Missing Write Protection for Parametric Data Values	1400	2199
HasMember	B	1315	Improper Setting of Bus Controlling Capability in Fabric End-point	1400	2202
HasMember	B	1316	Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges	1400	2204
HasMember	B	1317	Improper Access Control in Fabric Bridge	1400	2206
HasMember	B	1320	Improper Protection for Outbound Error Messages and Alert Signals	1400	2214
HasMember	B	1323	Improper Management of Sensitive Trace Data	1400	2220
HasMember	B	1328	Security Version Number Mutable to Older Versions	1400	2229
HasMember	B	1334	Unauthorized Error Injection Can Degrade Hardware Redundancy	1400	2246
HasMember	C	1390	Weak Authentication	1400	2279
HasMember	C	1391	Use of Weak Credentials	1400	2281
HasMember	B	1392	Use of Default Credentials	1400	2284
HasMember	B	1393	Use of Default Password	1400	2286
HasMember	B	1394	Use of Default Cryptographic Key	1400	2288

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1397: Comprehensive Categorization: Comparison

Category ID : 1397

Summary

Weaknesses in this category are related to comparison.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	B	183	Permissive List of Allowed Inputs	1400	464
HasMember	C	185	Incorrect Regular Expression	1400	469
HasMember	B	186	Overly Restrictive Regular Expression	1400	472

Nature	Type	ID	Name	V	Page
HasMember	V	187	Partial String Comparison	1400	474
HasMember	B	478	Missing Default Case in Multiple Condition Expression	1400	1149
HasMember	V	486	Comparison of Classes by Name	1400	1172
HasMember	V	595	Comparison of Object References Instead of Object Contents	1400	1342
HasMember	V	597	Use of Wrong Operator in String Comparison	1400	1345
HasMember	B	625	Permissive Regular Expression	1400	1400
HasMember	P	697	Incorrect Comparison	1400	1538
HasMember	V	777	Regular Expression without Anchors	1400	1645
HasMember	B	839	Numeric Range Comparison Without Minimum Check	1400	1776
HasMember	C	1023	Incomplete Comparison with Missing Factors	1400	1874
HasMember	B	1024	Comparison of Incompatible Types	1400	1877
HasMember	B	1025	Comparison Using Wrong Factors	1400	1878
HasMember	V	1077	Floating Point Comparison with Incorrect Operator	1400	1926

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1398: Comprehensive Categorization: Component Interaction

Category ID : 1398

Summary

Weaknesses in this category are related to component interaction.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	14	Compiler Removal of Code to Clear Buffers	1400	14
HasMember	B	115	Misinterpretation of Input	1400	286
HasMember	P	435	Improper Interaction Between Multiple Correctly-Behaving Entities	1400	1063
HasMember	C	436	Interpretation Conflict	1400	1065
HasMember	B	437	Incomplete Model of Endpoint Features	1400	1067
HasMember	B	439	Behavioral Change in New Version or Environment	1400	1068
HasMember	B	444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	1400	1075
HasMember	V	650	Trusting HTTP Permission Methods on the Server Side	1400	1441
HasMember	B	733	Compiler Optimization Removal or Modification of Security-critical Code	1400	1570
HasMember	B	1037	Processor Optimization Removal or Modification of Security-critical Code	1400	1879
HasMember	C	1038	Insecure Automated Optimizations	1400	1881

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1399: Comprehensive Categorization: Memory Safety

Category ID : 1399

Summary

Weaknesses in this category are related to memory safety.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1400	299
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1400	310
HasMember	V	121	Stack-based Buffer Overflow	1400	320
HasMember	V	122	Heap-based Buffer Overflow	1400	324
HasMember	B	123	Write-what-where Condition	1400	329
HasMember	B	124	Buffer Underwrite ('Buffer Underflow')	1400	332
HasMember	B	125	Out-of-bounds Read	1400	336
HasMember	V	126	Buffer Over-read	1400	340
HasMember	V	127	Buffer Under-read	1400	343
HasMember	V	129	Improper Validation of Array Index	1400	347
HasMember	B	131	Incorrect Calculation of Buffer Size	1400	361
HasMember	B	134	Use of Externally-Controlled Format String	1400	371
HasMember	B	188	Reliance on Data/Memory Layout	1400	476
HasMember	V	198	Use of Incorrect Byte Ordering	1400	510
HasMember	V	244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	1400	598
HasMember	V	401	Missing Release of Memory after Effective Lifetime	1400	980
HasMember	V	415	Double Free	1400	1015
HasMember	V	416	Use After Free	1400	1019
HasMember	B	466	Return of Pointer Value Outside of Expected Range	1400	1117
HasMember	B	562	Return of Stack Variable Address	1400	1287
HasMember	V	587	Assignment of a Fixed Address to a Pointer	1400	1330
HasMember	V	590	Free of Memory not on the Heap	1400	1335
HasMember	CO	680	Integer Overflow to Buffer Overflow	1400	1502
HasMember	CO	690	Unchecked Return Value to NULL Pointer Dereference	1400	1523
HasMember	V	761	Free of Pointer not at Start of Buffer	1400	1601
HasMember	V	762	Mismatched Memory Management Routines	1400	1605
HasMember	B	763	Release of Invalid Pointer or Reference	1400	1608
HasMember	B	786	Access of Memory Location Before Start of Buffer	1400	1666
HasMember	B	787	Out-of-bounds Write	1400	1669
HasMember	B	788	Access of Memory Location After End of Buffer	1400	1678
HasMember	V	789	Memory Allocation with Excessive Size Value	1400	1683
HasMember	B	805	Buffer Access with Incorrect Length Value	1400	1711
HasMember	V	806	Buffer Access Using Size of Source Buffer	1400	1719
HasMember	B	822	Untrusted Pointer Dereference	1400	1732
HasMember	B	823	Use of Out-of-range Pointer Offset	1400	1735
HasMember	B	824	Access of Uninitialized Pointer	1400	1738
HasMember	B	825	Expired Pointer Dereference	1400	1741

References

[REF-1328]National Security Agency. "Software Memory Safety". 2022 November 0. < https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF >.2023-04-25.

[REF-1329]Prossimo. "What is memory safety and why does it matter?". < https://www.memorysafety.org/docs/memory-safety/ >.2023-04-25.

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1401: Comprehensive Categorization: Concurrency

Category ID : 1401

Summary

Weaknesses in this category are related to concurrency.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1400	895
HasMember	B	363	Race Condition Enabling Link Following	1400	904
HasMember	B	364	Signal Handler Race Condition	1400	905
HasMember	B	366	Race Condition within a Thread	1400	910
HasMember	B	367	Time-of-check Time-of-use (TOCTOU) Race Condition	1400	913
HasMember	B	368	Context Switching Race Condition	1400	918
HasMember	B	412	Unrestricted Externally Accessible Lock	1400	1007
HasMember	B	413	Improper Resource Locking	1400	1010
HasMember	B	414	Missing Lock Check	1400	1014
HasMember	B	432	Dangerous Signal Handler not Disabled During Sensitive Operations	1400	1052
HasMember	V	479	Signal Handler Use of a Non-reentrant Function	1400	1154
HasMember	V	543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	1400	1263
HasMember	V	558	Use of getlogin() in Multithreaded Application	1400	1281
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	1400	1296
HasMember	V	572	Call to Thread run() instead of start()	1400	1305
HasMember	V	574	EJB Bad Practices: Use of Synchronization Primitives	1400	1308
HasMember	V	591	Sensitive Data Storage in Improperly Locked Memory	1400	1338
HasMember	B	609	Double-Checked Locking	1400	1371
HasMember	B	663	Use of a Non-reentrant Function in a Concurrent Context	1400	1461
HasMember	C	667	Improper Locking	1400	1472
HasMember	F	689	Permission Race Condition During Resource Copy	1400	1521
HasMember	B	764	Multiple Locks of a Critical Resource	1400	1613
HasMember	B	765	Multiple Unlocks of a Critical Resource	1400	1614
HasMember	B	820	Missing Synchronization	1400	1729
HasMember	B	821	Incorrect Synchronization	1400	1731

Nature	Type	ID	Name	V	Page
HasMember	V	828	Signal Handler with Functionality that is not Asynchronous-Safe	1400	1746
HasMember	V	831	Signal Handler Function Associated with Multiple Signals	1400	1758
HasMember	B	832	Unlock of a Resource that is not Locked	1400	1761
HasMember	B	833	Deadlock	1400	1762
HasMember	B	1058	Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element	1400	1903
HasMember	B	1088	Synchronous Access of Remote Resource without Timeout	1400	1937
HasMember	V	1096	Singleton Class Instance Creation without Proper Locking or Synchronization	1400	1945
HasMember	B	1223	Race Condition for Write-Once Attributes	1400	2011
HasMember	B	1232	Improper Lock Behavior After Power State Transition	1400	2021
HasMember	B	1234	Hardware Internal or Debug Modes Allow Override of Locks	1400	2026
HasMember	B	1264	Hardware Logic with Insecure De-Synchronization between Control and Data Channels	1400	2098
HasMember	B	1298	Hardware Logic Contains Race Conditions	1400	2170

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1402: Comprehensive Categorization: Encryption

Category ID : 1402

Summary

Weaknesses in this category are related to encryption.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	5	J2EE Misconfiguration: Data Transmission Without Encryption	1400	1
HasMember	C	311	Missing Encryption of Sensitive Data	1400	764
HasMember	B	312	Cleartext Storage of Sensitive Information	1400	771
HasMember	V	313	Cleartext Storage in a File or on Disk	1400	777
HasMember	V	314	Cleartext Storage in the Registry	1400	779
HasMember	V	315	Cleartext Storage of Sensitive Information in a Cookie	1400	781
HasMember	V	316	Cleartext Storage of Sensitive Information in Memory	1400	782
HasMember	V	317	Cleartext Storage of Sensitive Information in GUI	1400	784
HasMember	V	318	Cleartext Storage of Sensitive Information in Executable	1400	785
HasMember	B	319	Cleartext Transmission of Sensitive Information	1400	786
HasMember	B	324	Use of a Key Past its Expiration Date	1400	799
HasMember	B	325	Missing Cryptographic Step	1400	801
HasMember	C	326	Inadequate Encryption Strength	1400	803
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1400	806

Nature	Type	ID	Name	V	Page
HasMember	B	328	Use of Weak Hash	1400	813
HasMember	B	347	Improper Verification of Cryptographic Signature	1400	864
HasMember	V	614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	1400	1382
HasMember	V	759	Use of a One-Way Hash without a Salt	1400	1593
HasMember	V	760	Use of a One-Way Hash with a Predictable Salt	1400	1598
HasMember	V	780	Use of RSA Algorithm without OAEP	1400	1652
HasMember	B	916	Use of Password Hash With Insufficient Computational Effort	1400	1822
HasMember	B	1240	Use of a Cryptographic Primitive with a Risky Implementation	1400	2036

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1403: Comprehensive Categorization: Exposed Resource

Category ID : 1403

Summary

Weaknesses in this category are related to exposed resource.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	8	J2EE Misconfiguration: Entity Bean Declared Remote	1400	6
HasMember	B	15	External Control of System or Configuration Setting	1400	17
HasMember	B	73	External Control of File Name or Path	1400	133
HasMember	C	114	Process Control	1400	283
HasMember	V	219	Storage of File with Sensitive Data Under Web Root	1400	560
HasMember	V	220	Storage of File With Sensitive Data Under FTP Root	1400	562
HasMember	B	374	Passing Mutable Objects to an Untrusted Method	1400	927
HasMember	B	375	Returning a Mutable Object to an Untrusted Caller	1400	930
HasMember	C	377	Insecure Temporary File	1400	932
HasMember	B	378	Creation of Temporary File With Insecure Permissions	1400	935
HasMember	B	379	Creation of Temporary File in Directory with Insecure Permissions	1400	937
HasMember	C	402	Transmission of Private Resources into a New Sphere ('Resource Leak')	1400	984
HasMember	B	403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	1400	985
HasMember	B	426	Untrusted Search Path	1400	1035
HasMember	B	427	Uncontrolled Search Path Element	1400	1040
HasMember	B	428	Unquoted Search Path or Element	1400	1047
HasMember	V	433	Unparsed Raw Web Content Delivery	1400	1053
HasMember	B	472	External Control of Assumed-Immutable Web Parameter	1400	1131
HasMember	B	488	Exposure of Data Element to Wrong Session	1400	1176

Nature	Type	ID	Name	V	Page
HasMember	V	491	Public cloneable() Method Without Final ('Object Hijack')	1400	1181
HasMember	V	492	Use of Inner Class Containing Sensitive Data	1400	1183
HasMember	V	493	Critical Public Variable Without Final Modifier	1400	1190
HasMember	V	498	Cloneable Class Containing Sensitive Information	1400	1204
HasMember	V	499	Serializable Class Containing Sensitive Data	1400	1206
HasMember	V	500	Public Static Field Not Marked Final	1400	1208
HasMember	B	524	Use of Cache Containing Sensitive Information	1400	1240
HasMember	V	525	Use of Web Browser Cache Containing Sensitive Information	1400	1242
HasMember	V	527	Exposure of Version-Control Repository to an Unauthorized Control Sphere	1400	1245
HasMember	V	528	Exposure of Core Dump File to an Unauthorized Control Sphere	1400	1246
HasMember	V	529	Exposure of Access Control List Files to an Unauthorized Control Sphere	1400	1247
HasMember	V	530	Exposure of Backup File to an Unauthorized Control Sphere	1400	1248
HasMember	V	539	Use of Persistent Cookies Containing Sensitive Information	1400	1259
HasMember	B	552	Files or Directories Accessible to External Parties	1400	1274
HasMember	V	553	Command Shell in Externally Accessible Directory	1400	1277
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	1400	1292
HasMember	V	582	Array Declared Public, Final, and Static	1400	1322
HasMember	V	583	finalize() Method Declared Public	1400	1324
HasMember	V	608	Struts: Non-private Field in ActionForm Class	1400	1369
HasMember	B	619	Dangling Database Cursor ('Cursor Injection')	1400	1391
HasMember	C	642	External Control of Critical State Data	1400	1422
HasMember	C	668	Exposure of Resource to Wrong Sphere	1400	1478
HasMember	B	767	Access to Critical Private Variable via Public Method	1400	1619
HasMember	V	784	Reliance on Cookies without Validation and Integrity Checking in a Security Decision	1400	1662
HasMember	B	1282	Assumed-Immutable Data is Stored in Writable Memory	1400	2139
HasMember	B	1327	Binding to an Unrestricted IP Address	1400	2227

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1404: Comprehensive Categorization: File Handling

Category ID : 1404

Summary

Weaknesses in this category are related to file handling.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619

Nature	Type	ID	Name	V	Page
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1400	33
HasMember	B	23	Relative Path Traversal	1400	46
HasMember	V	24	Path Traversal: '../filedir'	1400	53
HasMember	V	25	Path Traversal: '/../filedir'	1400	55
HasMember	V	26	Path Traversal: '/dir/../filename'	1400	57
HasMember	V	27	Path Traversal: 'dir/../../filename'	1400	58
HasMember	V	28	Path Traversal: '..\filedir'	1400	60
HasMember	V	29	Path Traversal: '\..\filename'	1400	62
HasMember	V	30	Path Traversal: '\dir\..\filename'	1400	64
HasMember	V	31	Path Traversal: 'dir\..\..\filename'	1400	65
HasMember	V	32	Path Traversal: '...' (Triple Dot)	1400	67
HasMember	V	33	Path Traversal: '....' (Multiple Dot)	1400	69
HasMember	V	34	Path Traversal: '....//'	1400	71
HasMember	V	35	Path Traversal: '.../...//'	1400	73
HasMember	B	36	Absolute Path Traversal	1400	75
HasMember	V	37	Path Traversal: '/absolute/pathname/here'	1400	79
HasMember	V	38	Path Traversal: '\absolute\pathname\here'	1400	81
HasMember	V	39	Path Traversal: 'C:dirname'	1400	83
HasMember	V	40	Path Traversal: '\\UNC\share\name\' (Windows UNC Share)	1400	86
HasMember	B	41	Improper Resolution of Path Equivalence	1400	87
HasMember	V	42	Path Equivalence: 'filename.' (Trailing Dot)	1400	93
HasMember	V	43	Path Equivalence: 'filename....' (Multiple Trailing Dot)	1400	94
HasMember	V	44	Path Equivalence: 'file.name' (Internal Dot)	1400	95
HasMember	V	45	Path Equivalence: 'file...name' (Multiple Internal Dot)	1400	96
HasMember	V	46	Path Equivalence: 'filename ' (Trailing Space)	1400	97
HasMember	V	47	Path Equivalence: ' filename' (Leading Space)	1400	98
HasMember	V	48	Path Equivalence: 'file name' (Internal Whitespace)	1400	99
HasMember	V	49	Path Equivalence: 'filename/' (Trailing Slash)	1400	100
HasMember	V	50	Path Equivalence: '//multiple/leading/slash'	1400	101
HasMember	V	51	Path Equivalence: '/multiple//internal/slash'	1400	103
HasMember	V	52	Path Equivalence: '/multiple/trailing/slash//'	1400	104
HasMember	V	53	Path Equivalence: '\multiple\\internal\backslash'	1400	105
HasMember	V	54	Path Equivalence: 'filedir\' (Trailing Backslash)	1400	106
HasMember	V	55	Path Equivalence: '/./' (Single Dot Directory)	1400	107
HasMember	V	56	Path Equivalence: 'filedir*' (Wildcard)	1400	108
HasMember	V	57	Path Equivalence: 'fakedir/../realdir/filename'	1400	109
HasMember	V	58	Path Equivalence: Windows 8.3 Filename	1400	111
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	1400	112
HasMember	C	61	UNIX Symbolic Link (Symlink) Following	1400	117
HasMember	V	62	UNIX Hard Link	1400	120
HasMember	V	64	Windows Shortcut Following (.LNK)	1400	122
HasMember	V	65	Windows Hard Link	1400	124
HasMember	B	66	Improper Handling of File Names that Identify Virtual Resources	1400	125
HasMember	V	67	Improper Handling of Windows Device Names	1400	127

Nature	Type	ID	Name	V	Page
HasMember	V	69	Improper Handling of Windows ::DATA Alternate Data Stream	1400	130
HasMember	V	72	Improper Handling of Apple HFS+ Alternate Data Stream Path	1400	131

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1405: Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions

Category ID : 1405

Summary

Weaknesses in this category are related to improper check or handling of exceptional conditions.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	7	J2EE Misconfiguration: Missing Custom Error Page	1400	4
HasMember	V	12	ASP.NET Misconfiguration: Missing Custom Error Page	1400	11
HasMember	B	252	Unchecked Return Value	1400	613
HasMember	B	390	Detection of Error Condition Without Action	1400	950
HasMember	B	391	Unchecked Error Condition	1400	955
HasMember	B	394	Unexpected Status Code or Return Value	1400	962
HasMember	B	544	Missing Standardized Error Handling Mechanism	1400	1265
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1400	1544
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1400	1577
HasMember	C	755	Improper Handling of Exceptional Conditions	1400	1585
HasMember	B	756	Missing Custom Error Page	1400	1588
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1400	2056
HasMember	B	1261	Improper Handling of Single Event Upsets	1400	2091
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1400	2240
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1400	2265
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1400	2269

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1406: Comprehensive Categorization: Improper Input Validation

Category ID : 1406

Summary

Weaknesses in this category are related to improper input validation.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	20	Improper Input Validation	1400	20
HasMember	V	105	Struts: Form Field Without Validator	1400	259
HasMember	V	106	Struts: Plug-in Framework not in Use	1400	262
HasMember	V	108	Struts: Unvalidated Action Form	1400	267
HasMember	V	109	Struts: Validator Turned Off	1400	269
HasMember	B	112	Missing XML Validation	1400	275
HasMember	V	554	ASP.NET Misconfiguration: Not Using Input Validation Framework	1400	1278
HasMember	B	606	Unchecked Input for Loop Condition	1400	1366
HasMember	V	622	Improper Validation of Function Hook Arguments	1400	1396
HasMember	V	781	Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code	1400	1654
HasMember	B	1173	Improper Use of Validation Framework	1400	1978
HasMember	V	1174	ASP.NET Misconfiguration: Improper Model Validation	1400	1979
HasMember	B	1284	Improper Validation of Specified Quantity in Input	1400	2142
HasMember	B	1285	Improper Validation of Specified Index, Position, or Offset in Input	1400	2144
HasMember	B	1286	Improper Validation of Syntactic Correctness of Input	1400	2148
HasMember	B	1287	Improper Validation of Specified Type of Input	1400	2150
HasMember	B	1288	Improper Validation of Consistency within Input	1400	2151
HasMember	B	1289	Improper Validation of Unsafe Equivalence in Input	1400	2153

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1407: Comprehensive Categorization: Improper Neutralization

Category ID : 1407

Summary

Weaknesses in this category are related to improper neutralization.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	116	Improper Encoding or Escaping of Output	1400	287
HasMember	B	117	Improper Output Neutralization for Logs	1400	294
HasMember	B	130	Improper Handling of Length Parameter Inconsistency	1400	357
HasMember	C	138	Improper Neutralization of Special Elements	1400	379
HasMember	B	140	Improper Neutralization of Delimiters	1400	382
HasMember	V	141	Improper Neutralization of Parameter/Argument Delimiters	1400	384

Nature	Type	ID	Name	V	Page
HasMember	V	142	Improper Neutralization of Value Delimiters	1400	386
HasMember	V	143	Improper Neutralization of Record Delimiters	1400	387
HasMember	V	144	Improper Neutralization of Line Delimiters	1400	389
HasMember	V	145	Improper Neutralization of Section Delimiters	1400	391
HasMember	V	146	Improper Neutralization of Expression/Command Delimiters	1400	393
HasMember	V	147	Improper Neutralization of Input Terminators	1400	395
HasMember	V	148	Improper Neutralization of Input Leaders	1400	397
HasMember	V	149	Improper Neutralization of Quoting Syntax	1400	398
HasMember	V	150	Improper Neutralization of Escape, Meta, or Control Sequences	1400	400
HasMember	V	151	Improper Neutralization of Comment Delimiters	1400	402
HasMember	V	152	Improper Neutralization of Macro Symbols	1400	404
HasMember	V	153	Improper Neutralization of Substitution Characters	1400	406
HasMember	V	154	Improper Neutralization of Variable Name Delimiters	1400	407
HasMember	V	155	Improper Neutralization of Wildcards or Matching Symbols	1400	409
HasMember	V	156	Improper Neutralization of Whitespace	1400	411
HasMember	V	157	Failure to Sanitize Paired Delimiters	1400	413
HasMember	V	158	Improper Neutralization of Null Byte or NUL Character	1400	415
HasMember	C	159	Improper Handling of Invalid Use of Special Elements	1400	417
HasMember	V	160	Improper Neutralization of Leading Special Elements	1400	419
HasMember	V	161	Improper Neutralization of Multiple Leading Special Elements	1400	421
HasMember	V	162	Improper Neutralization of Trailing Special Elements	1400	423
HasMember	V	163	Improper Neutralization of Multiple Trailing Special Elements	1400	425
HasMember	V	164	Improper Neutralization of Internal Special Elements	1400	426
HasMember	V	165	Improper Neutralization of Multiple Internal Special Elements	1400	428
HasMember	B	166	Improper Handling of Missing Special Element	1400	429
HasMember	B	167	Improper Handling of Additional Special Element	1400	431
HasMember	B	168	Improper Handling of Inconsistent Special Elements	1400	433
HasMember	B	170	Improper Null Termination	1400	434
HasMember	C	172	Encoding Error	1400	439
HasMember	V	173	Improper Handling of Alternate Encoding	1400	441
HasMember	V	174	Double Decoding of the Same Data	1400	443
HasMember	V	175	Improper Handling of Mixed Encoding	1400	445
HasMember	V	176	Improper Handling of Unicode Encoding	1400	446
HasMember	V	177	Improper Handling of URL Encoding (Hex Encoding)	1400	449
HasMember	C	228	Improper Handling of Syntactically Invalid Structure	1400	575
HasMember	B	229	Improper Handling of Values	1400	577
HasMember	V	230	Improper Handling of Missing Values	1400	578
HasMember	V	231	Improper Handling of Extra Values	1400	579
HasMember	V	232	Improper Handling of Undefined Values	1400	580
HasMember	B	233	Improper Handling of Parameters	1400	581
HasMember	V	234	Failure to Handle Missing Parameter	1400	583
HasMember	V	235	Improper Handling of Extra Parameters	1400	585
HasMember	V	236	Improper Handling of Undefined Parameters	1400	586

Nature	Type	ID	Name	V	Page
HasMember	B	237	Improper Handling of Structural Elements	1400	587
HasMember	V	238	Improper Handling of Incomplete Structural Elements	1400	588
HasMember	V	239	Failure to Handle Incomplete Element	1400	589
HasMember	B	240	Improper Handling of Inconsistent Structural Elements	1400	590
HasMember	B	241	Improper Handling of Unexpected Data Type	1400	591
HasMember	B	463	Deletion of Data Structure Sentinel	1400	1113
HasMember	B	464	Addition of Data Structure Sentinel	1400	1115
HasMember	V	626	Null Byte Interaction Error (Poison Null Byte)	1400	1403
HasMember	V	644	Improper Neutralization of HTTP Headers for Scripting Syntax	1400	1430
HasMember	P	707	Improper Neutralization	1400	1554
HasMember	C	790	Improper Filtering of Special Elements	1400	1687
HasMember	B	791	Incomplete Filtering of Special Elements	1400	1689
HasMember	V	792	Incomplete Filtering of One or More Instances of Special Elements	1400	1690
HasMember	V	793	Only Filtering One Instance of a Special Element	1400	1692
HasMember	V	794	Incomplete Filtering of Multiple Instances of Special Elements	1400	1693
HasMember	B	795	Only Filtering Special Elements at a Specified Location	1400	1694
HasMember	V	796	Only Filtering Special Elements Relative to a Marker	1400	1696
HasMember	V	797	Only Filtering Special Elements at an Absolute Position	1400	1698
HasMember	B	838	Inappropriate Encoding for Output Context	1400	1773

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1408: Comprehensive Categorization: Incorrect Calculation

Category ID : 1408

Summary

Weaknesses in this category are related to incorrect calculation.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	B	128	Wrap-around Error	1400	345
HasMember	B	135	Incorrect Calculation of Multi-Byte String Length	1400	377
HasMember	B	190	Integer Overflow or Wraparound	1400	478
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	1400	487
HasMember	B	193	Off-by-one Error	1400	493
HasMember	B	369	Divide By Zero	1400	920
HasMember	V	467	Use of sizeof() on a Pointer Type	1400	1118
HasMember	B	468	Incorrect Pointer Scaling	1400	1121
HasMember	B	469	Use of Pointer Subtraction to Determine Size	1400	1123
HasMember	P	682	Incorrect Calculation	1400	1507
HasMember	B	1335	Incorrect Bitwise Shift of Integer	1400	2247

Nature	Type	ID	Name	V	Page
HasMember	B	1339	Insufficient Precision or Accuracy of a Real Number	1400	2254

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1409: Comprehensive Categorization: Injection

Category ID : 1409

Summary

Weaknesses in this category are related to injection.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1400	138
HasMember	C	75	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)	1400	145
HasMember	B	76	Improper Neutralization of Equivalent Special Elements	1400	146
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1400	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1400	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1400	168
HasMember	V	80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	1400	182
HasMember	V	81	Improper Neutralization of Script in an Error Message Web Page	1400	184
HasMember	V	82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	1400	186
HasMember	V	83	Improper Neutralization of Script in Attributes in a Web Page	1400	188
HasMember	V	84	Improper Neutralization of Encoded URI Schemes in a Web Page	1400	190
HasMember	V	85	Doubled Character XSS Manipulations	1400	192
HasMember	V	86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	1400	194
HasMember	V	87	Improper Neutralization of Alternate XSS Syntax	1400	196
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1400	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1400	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	1400	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	1400	220
HasMember	B	93	Improper Neutralization of CRLF Sequences ('CRLF Injection')	1400	222

Nature	Type	ID	Name	V	Page
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	1400	225
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	1400	232
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	1400	238
HasMember	V	97	Improper Neutralization of Server-Side Includes (SSI) Within a Web Page	1400	241
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	1400	249
HasMember	V	102	Struts: Duplicate Validation Forms	1400	252
HasMember	V	113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')	1400	277
HasMember	V	564	SQL Injection: Hibernate	1400	1290
HasMember	V	621	Variable Extraction Error	1400	1394
HasMember	B	624	Executable Regular Expression Error	1400	1399
HasMember	V	627	Dynamic Variable Evaluation	1400	1405
HasMember	B	641	Improper Restriction of Names for Files and Other Resources	1400	1421
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1400	1428
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1400	1444
HasMember	∞	692	Incomplete Denylist to Cross-Site Scripting	1400	1528
HasMember	B	694	Use of Multiple Resources with Duplicate Identifier	1400	1531
HasMember	B	914	Improper Control of Dynamically-Identified Variables	1400	1816
HasMember	B	917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	1400	1827
HasMember	C	943	Improper Neutralization of Special Elements in Data Query Logic	1400	1860
HasMember	B	1236	Improper Neutralization of Formula Elements in a CSV File	1400	2031
HasMember	B	1336	Improper Neutralization of Special Elements Used in a Template Engine	1400	2250
HasMember	B	1426	Improper Validation of Generative AI Output	1400	2321
HasMember	B	1427	Improper Neutralization of Input Used for LLM Prompting	1400	2324

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1410: Comprehensive Categorization: Insufficient Control Flow Management

Category ID : 1410

Summary

Weaknesses in this category are related to insufficient control flow management.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	B	179	Incorrect Behavior Order: Early Validation	1400	454
HasMember	V	180	Incorrect Behavior Order: Validate Before Canonicalize	1400	457
HasMember	V	181	Incorrect Behavior Order: Validate Before Filter	1400	460
HasMember	B	248	Uncaught Exception	1400	603
HasMember	V	382	J2EE Bad Practices: Use of System.exit()	1400	940
HasMember	B	395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	1400	964
HasMember	B	396	Declaration of Catch for Generic Exception	1400	966
HasMember	B	397	Declaration of Throws for Generic Exception	1400	968
HasMember	B	408	Incorrect Behavior Order: Early Amplification	1400	1002
HasMember	B	430	Deployment of Wrong Handler	1400	1049
HasMember	B	431	Missing Handler	1400	1051
HasMember	B	455	Non-exit on Failed Initialization	1400	1095
HasMember	B	480	Use of Incorrect Operator	1400	1157
HasMember	V	481	Assigning instead of Comparing	1400	1161
HasMember	V	482	Comparing instead of Assigning	1400	1165
HasMember	B	483	Incorrect Block Delimitation	1400	1167
HasMember	B	584	Return Inside Finally Block	1400	1325
HasMember	V	600	Uncaught Exception in Servlet	1400	1352
HasMember	B	617	Reachable Assertion	1400	1387
HasMember	C	670	Always-Incorrect Control Flow Implementation	1400	1484
HasMember	C	674	Uncontrolled Recursion	1400	1493
HasMember	P	691	Insufficient Control Flow Management	1400	1525
HasMember	C	696	Incorrect Behavior Order	1400	1535
HasMember	B	698	Execution After Redirect (EAR)	1400	1542
HasMember	C	705	Incorrect Control Flow Scoping	1400	1550
HasMember	V	768	Incorrect Short Circuit Evaluation	1400	1620
HasMember	B	783	Operator Precedence Logic Error	1400	1659
HasMember	C	799	Improper Control of Interaction Frequency	1400	1708
HasMember	C	834	Excessive Iteration	1400	1763
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1400	1766
HasMember	B	837	Improper Enforcement of a Single, Unique Action	1400	1771
HasMember	B	841	Improper Enforcement of Behavioral Workflow	1400	1781
HasMember	B	1190	DMA Device Enabled Too Early in Boot Phase	1400	1987
HasMember	B	1193	Power-On of Untrusted Execution Core Before Enabling Fabric Access Control	1400	1995
HasMember	B	1265	Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls	1400	2100
HasMember	B	1280	Access Control Check Implemented After Asset is Accessed	1400	2134
HasMember	B	1281	Sequence of Processor Instructions Leads to Unexpected Behavior	1400	2136
HasMember	B	1322	Use of Blocking Code in Single-threaded, Non-blocking Context	1400	2219

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1411: Comprehensive Categorization: Insufficient Verification of Data Authenticity

Category ID : 1411

Summary

Weaknesses in this category are related to insufficient verification of data authenticity.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	345	Insufficient Verification of Data Authenticity	1400	858
HasMember	C	346	Origin Validation Error	1400	860
HasMember	B	348	Use of Less Trusted Source	1400	866
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1400	868
HasMember	B	351	Insufficient Type Distinction	1400	873
HasMember	B	352	Cross-Site Request Forgery (CSRF)	1400	875
HasMember	B	353	Missing Support for Integrity Check	1400	881
HasMember	B	354	Improper Validation of Integrity Check Value	1400	883
HasMember	B	360	Trust of System Event Data	1400	894
HasMember	B	494	Download of Code Without Integrity Check	1400	1192
HasMember	V	616	Incomplete Identification of Uploaded File Variables (PHP)	1400	1385
HasMember	V	646	Reliance on File Name or Extension of Externally-Supplied File	1400	1434
HasMember	B	649	Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking	1400	1439
HasMember	B	924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel	1400	1839
HasMember	B	1293	Missing Source Correlation of Multiple Independent Data	1400	2161
HasMember	V	1385	Missing Origin Validation in WebSockets	1400	2271

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1412: Comprehensive Categorization: Poor Coding Practices

Category ID : 1412

Summary

Weaknesses in this category are related to poor coding practices.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	11	ASP.NET Misconfiguration: Creating Debug Binary	1400	9
HasMember	V	103	Struts: Incomplete validate() Method Definition	1400	254
HasMember	V	104	Struts: Form Bean Does Not Extend Validation Class	1400	257
HasMember	V	107	Struts: Unused Validation Form	1400	265
HasMember	V	110	Struts: Validator Without Form Field	1400	270
HasMember	V	111	Direct Use of Unsafe JNI	1400	272
HasMember	B	242	Use of Inherently Dangerous Function	1400	593
HasMember	V	245	J2EE Bad Practices: Direct Management of Connections	1400	599
HasMember	V	246	J2EE Bad Practices: Direct Use of Sockets	1400	601
HasMember	B	253	Incorrect Check of Function Return Value	1400	620
HasMember	B	358	Improperly Implemented Security Check for Standard	1400	888
HasMember	V	383	J2EE Bad Practices: Direct Use of Threads	1400	942
HasMember	B	392	Missing Report of Error Condition	1400	958
HasMember	B	393	Return of Wrong Status Code	1400	960
HasMember	B	440	Expected Behavior Violation	1400	1069
HasMember	C	446	UI Discrepancy for Security Feature	1400	1081
HasMember	B	448	Obsolete Feature in UI	1400	1083
HasMember	B	449	The UI Performs the Wrong Action	1400	1084
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1400	1087
HasMember	V	462	Duplicate Key in Associative List (Alist)	1400	1111
HasMember	B	474	Use of Function with Inconsistent Implementations	1400	1136
HasMember	B	475	Undefined Behavior for Input to API	1400	1138
HasMember	B	476	NULL Pointer Dereference	1400	1139
HasMember	B	477	Use of Obsolete Function	1400	1146
HasMember	B	484	Omitted Break Statement in Switch	1400	1169
HasMember	B	489	Active Debug Code	1400	1178
HasMember	C	506	Embedded Malicious Code	1400	1218
HasMember	B	507	Trojan Horse	1400	1220
HasMember	B	508	Non-Replicating Malicious Code	1400	1221
HasMember	B	509	Replicating Malicious Code (Virus or Worm)	1400	1222
HasMember	B	510	Trapdoor	1400	1223
HasMember	B	511	Logic/Time Bomb	1400	1225
HasMember	B	512	Spyware	1400	1226
HasMember	V	546	Suspicious Comment	1400	1266
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	1400	1267
HasMember	V	560	Use of umask() with chmod-style Argument	1400	1282
HasMember	B	561	Dead Code	1400	1283
HasMember	B	563	Assignment to Variable without Use	1400	1289
HasMember	B	570	Expression is Always False	1400	1300
HasMember	B	571	Expression is Always True	1400	1303
HasMember	C	573	Improper Following of Specification by Caller	1400	1307
HasMember	V	575	EJB Bad Practices: Use of AWT Swing	1400	1310
HasMember	V	576	EJB Bad Practices: Use of Java I/O	1400	1312
HasMember	V	577	EJB Bad Practices: Use of Sockets	1400	1314
HasMember	V	578	EJB Bad Practices: Use of Class Loader	1400	1316

Nature	Type	ID	Name	V	Page
HasMember	V	579	J2EE Bad Practices: Non-serializable Object Stored in Session	1400	1318
HasMember	V	581	Object Model Violation: Just One of Equals and Hashcode Defined	1400	1321
HasMember	V	585	Empty Synchronized Block	1400	1327
HasMember	B	586	Explicit Call to Finalize()	1400	1329
HasMember	V	589	Call to Non-ubiquitous API	1400	1333
HasMember	V	594	J2EE Framework: Saving Unserializable Objects to Disk	1400	1341
HasMember	V	605	Multiple Binds to the Same Port	1400	1364
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1400	1407
HasMember	C	675	Multiple Operations on Resource in Single-Operation Context	1400	1496
HasMember	B	676	Use of Potentially Dangerous Function	1400	1498
HasMember	V	683	Function Call With Incorrect Order of Arguments	1400	1512
HasMember	C	684	Incorrect Provision of Specified Functionality	1400	1514
HasMember	V	685	Function Call With Incorrect Number of Arguments	1400	1516
HasMember	V	686	Function Call With Incorrect Argument Type	1400	1517
HasMember	V	687	Function Call With Incorrectly Specified Argument Value	1400	1518
HasMember	V	688	Function Call With Incorrect Variable or Reference as Argument	1400	1520
HasMember	B	695	Use of Low-Level Functionality	1400	1533
HasMember	P	710	Improper Adherence to Coding Standards	1400	1558
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1400	1591
HasMember	B	766	Critical Data Element Declared Public	1400	1615
HasMember	V	785	Use of Path Manipulation Function without Maximum-sized Buffer	1400	1664
HasMember	C	912	Hidden Functionality	1400	1812
HasMember	B	1007	Insufficient Visual Distinction of Homoglyphs Presented to User	1400	1866
HasMember	B	1041	Use of Redundant Code	1400	1884
HasMember	B	1043	Data Element Aggregating an Excessively Large Number of Non-Primitive Elements	1400	1887
HasMember	B	1044	Architecture with Number of Horizontal Layers Outside of Expected Range	1400	1888
HasMember	B	1045	Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor	1400	1889
HasMember	B	1047	Modules with Circular Dependencies	1400	1891
HasMember	B	1048	Invokable Control Element with Large Number of Outward Calls	1400	1892
HasMember	B	1053	Missing Documentation for Design	1400	1898
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer	1400	1899
HasMember	B	1055	Multiple Inheritance from Concrete Classes	1400	1900
HasMember	B	1056	Invokable Control Element with Variadic Parameters	1400	1901
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component	1400	1902
HasMember	C	1059	Insufficient Technical Documentation	1400	1904
HasMember	B	1060	Excessive Number of Inefficient Server-Side Data Accesses	1400	1906
HasMember	C	1061	Insufficient Encapsulation	1400	1907

Nature	Type	ID	Name	V	Page
HasMember	B	1062	Parent Class with References to Child Class	1400	1909
HasMember	B	1064	Invokable Control Element with Signature Containing an Excessive Number of Parameters	1400	1911
HasMember	B	1065	Runtime Resource Management Control Element in a Component Built to Run on Application Servers	1400	1912
HasMember	B	1066	Missing Serialization Control Element	1400	1913
HasMember	B	1068	Inconsistency Between Implementation and Documented Design	1400	1915
HasMember	V	1069	Empty Exception Block	1400	1916
HasMember	B	1070	Serializable Data Element Containing non-Serializable Item Elements	1400	1918
HasMember	B	1071	Empty Code Block	1400	1919
HasMember	B	1074	Class with Excessively Deep Inheritance	1400	1923
HasMember	B	1075	Unconditional Control Flow Transfer outside of Switch Block	1400	1924
HasMember	C	1076	Insufficient Adherence to Expected Conventions	1400	1925
HasMember	C	1078	Inappropriate Source Code Style or Formatting	1400	1927
HasMember	B	1079	Parent Class without Virtual Destructor Method	1400	1929
HasMember	B	1080	Source Code File with Excessive Number of Lines of Code	1400	1930
HasMember	B	1082	Class Instance Self Destruction Control Element	1400	1931
HasMember	B	1083	Data Access from Outside Expected Data Manager Component	1400	1932
HasMember	B	1085	Invokable Control Element with Excessive Volume of Commented-out Code	1400	1934
HasMember	B	1086	Class with Excessive Number of Child Classes	1400	1935
HasMember	B	1087	Class with Virtual Method without a Virtual Destructor	1400	1936
HasMember	B	1090	Method Containing Access of a Member Element from Another Class	1400	1939
HasMember	B	1092	Use of Same Invokable Control Element in Multiple Architectural Layers	1400	1941
HasMember	C	1093	Excessively Complex Data Representation	1400	1942
HasMember	B	1095	Loop Condition Value Update within the Loop	1400	1944
HasMember	B	1097	Persistent Storable Data Element without Associated Comparison Control Element	1400	1946
HasMember	B	1098	Data Element containing Pointer Item without Proper Copy Control Element	1400	1947
HasMember	B	1099	Inconsistent Naming Conventions for Identifiers	1400	1948
HasMember	B	1100	Insufficient Isolation of System-Dependent Functions	1400	1949
HasMember	B	1101	Reliance on Runtime Component in Generated Code	1400	1950
HasMember	B	1102	Reliance on Machine-Dependent Data Representation	1400	1951
HasMember	B	1103	Use of Platform-Dependent Third Party Components	1400	1952
HasMember	B	1105	Insufficient Encapsulation of Machine-Dependent Functionality	1400	1954
HasMember	B	1106	Insufficient Use of Symbolic Constants	1400	1955
HasMember	B	1107	Insufficient Isolation of Symbolic Constant Definitions	1400	1956
HasMember	B	1108	Excessive Reliance on Global Variables	1400	1957
HasMember	B	1109	Use of Same Variable for Multiple Purposes	1400	1958
HasMember	B	1110	Incomplete Design Documentation	1400	1959
HasMember	B	1111	Incomplete I/O Documentation	1400	1960
HasMember	B	1112	Incomplete Documentation of Program Execution	1400	1961

Nature	Type	ID	Name	V	Page
HasMember	B	1113	Inappropriate Comment Style	1400	1962
HasMember	B	1114	Inappropriate Whitespace Style	1400	1963
HasMember	B	1115	Source Code Element without Standard Prologue	1400	1963
HasMember	B	1116	Inaccurate Comments	1400	1964
HasMember	B	1117	Callable with Insufficient Behavioral Summary	1400	1966
HasMember	B	1118	Insufficient Documentation of Error Handling Techniques	1400	1967
HasMember	B	1119	Excessive Use of Unconditional Branching	1400	1968
HasMember	C	1120	Excessive Code Complexity	1400	1969
HasMember	B	1121	Excessive McCabe Cyclomatic Complexity	1400	1970
HasMember	B	1122	Excessive Halstead Complexity	1400	1971
HasMember	B	1123	Excessive Use of Self-Modifying Code	1400	1972
HasMember	B	1124	Excessively Deep Nesting	1400	1973
HasMember	B	1125	Excessive Attack Surface	1400	1974
HasMember	B	1126	Declaration of Variable with Unnecessarily Wide Scope	1400	1975
HasMember	B	1127	Compilation with Insufficient Warnings or Errors	1400	1976
HasMember	C	1164	Irrelevant Code	1400	1976
HasMember	C	1177	Use of Prohibited Code	1400	1981
HasMember	B	1209	Failure to Disable Reserved Bits	1400	2000
HasMember	B	1245	Improper Finite State Machines (FSMs) in Hardware Logic	1400	2052
HasMember	B	1341	Multiple Releases of Same Resource or Handle	1400	2258
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1400	2266

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1413: Comprehensive Categorization: Protection Mechanism Failure

Category ID : 1413

Summary

Weaknesses in this category are related to protection mechanism failure.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	B	182	Collapse of Data into Unsafe Value	1400	462
HasMember	B	184	Incomplete List of Disallowed Inputs	1400	466
HasMember	B	222	Truncation of Security-relevant Information	1400	565
HasMember	B	223	Omission of Security-relevant Information	1400	566
HasMember	B	224	Obscured Security-relevant Information by Alternate Name	1400	568
HasMember	B	356	Product UI does not Warn User of Unsafe Actions	1400	886
HasMember	B	357	Insufficient UI Warning of Dangerous Operations	1400	887
HasMember	B	450	Multiple Interpretations of UI Input	1400	1085
HasMember	C	602	Client-Side Enforcement of Server-Side Security	1400	1359

Nature	Type	ID	Name	V	Page
HasMember	P	693	Protection Mechanism Failure	1400	1529
HasMember	B	757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')	1400	1589
HasMember	B	778	Insufficient Logging	1400	1647
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1400	1723
HasMember	C	1039	Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations	1400	1882
HasMember	B	1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications	1400	2060
HasMember	B	1253	Incorrect Selection of Fuse Values	1400	2069
HasMember	B	1269	Product Released in Non-Release Configuration	1400	2110
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1400	2131
HasMember	B	1291	Public Key Re-Use for Signing both Debug and Production Code	1400	2157
HasMember	B	1318	Missing Support for Security Features in On-chip Fabrics or Buses	1400	2209
HasMember	B	1319	Improper Protection against Electromagnetic Fault Injection (EM-FI)	1400	2212
HasMember	B	1326	Missing Immutable Root of Trust in Hardware	1400	2224
HasMember	B	1338	Improper Protections Against Hardware Overheating	1400	2252

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1414: Comprehensive Categorization: Randomness

Category ID : 1414

Summary

Weaknesses in this category are related to randomness.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	6	J2EE Misconfiguration: Insufficient Session-ID Length	1400	2
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	1400	797
HasMember	V	329	Generation of Predictable IV with CBC Mode	1400	818
HasMember	C	330	Use of Insufficiently Random Values	1400	821
HasMember	B	331	Insufficient Entropy	1400	828
HasMember	V	332	Insufficient Entropy in PRNG	1400	830
HasMember	V	333	Improper Handling of Insufficient Entropy in TRNG	1400	832
HasMember	B	334	Small Space of Random Values	1400	834
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	1400	836
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1400	839

Nature	Type	ID	Name	V	Page
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1400	841
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	1400	844
HasMember	V	339	Small Seed Space in PRNG	1400	847
HasMember	C	340	Generation of Predictable Numbers or Identifiers	1400	849
HasMember	B	341	Predictable from Observable State	1400	850
HasMember	B	342	Predictable Exact Value from Previous Values	1400	852
HasMember	B	343	Predictable Value Range from Previous Values	1400	854
HasMember	B	344	Use of Invariant Value in Dynamically Changing Context	1400	856
HasMember	B	1204	Generation of Weak Initialization Vector (IV)	1400	1996
HasMember	B	1241	Use of Predictable Algorithm in Random Number Generator	1400	2042

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1415: Comprehensive Categorization: Resource Control

Category ID : 1415

Summary

Weaknesses in this category are related to resource control.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	B	385	Covert Timing Channel	1400	947
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1400	1125
HasMember	V	473	PHP External Variable Modification	1400	1134
HasMember	B	502	Deserialization of Untrusted Data	1400	1212
HasMember	C	514	Covert Channel	1400	1227
HasMember	B	515	Covert Storage Channel	1400	1229
HasMember	C	672	Operation on a Resource after Expiration or Release	1400	1488
HasMember	B	826	Premature Release of Resource During Expected Lifetime	1400	1743
HasMember	B	910	Use of Expired File Descriptor	1400	1809
HasMember	B	915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	1400	1818
HasMember	B	1104	Use of Unmaintained Third Party Components	1400	1953
HasMember	B	1249	Application-Level Admin Tool with Inconsistent View of Underlying Operating System	1400	2062
HasMember	B	1251	Mirrored Regions with Different Values	1400	2065
HasMember	B	1277	Firmware Not Updateable	1400	2128
HasMember	B	1310	Missing Ability to Patch ROM Code	1400	2191
HasMember	V	1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	1400	2216

Nature	Type	ID	Name	V	Page
HasMember	B	1329	Reliance on Component That is Not Updateable	1400	2231

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1416: Comprehensive Categorization: Resource Lifecycle Management

Category ID : 1416

Summary

Weaknesses in this category are related to resource lifecycle management.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	V	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	1400	242
HasMember	C	118	Incorrect Access of Indexable Resource ('Range Error')	1400	298
HasMember	B	178	Improper Handling of Case Sensitivity	1400	451
HasMember	V	192	Integer Coercion Error	1400	489
HasMember	V	194	Unexpected Sign Extension	1400	498
HasMember	V	195	Signed to Unsigned Conversion Error	1400	501
HasMember	V	196	Unsigned to Signed Conversion Error	1400	505
HasMember	B	197	Numeric Truncation Error	1400	507
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	1400	551
HasMember	C	221	Information Loss or Omission	1400	563
HasMember	B	226	Sensitive Information in Resource Not Removed Before Reuse	1400	569
HasMember	V	243	Creation of chroot Jail Without Changing Working Directory	1400	596
HasMember	B	372	Incomplete Internal State Distinction	1400	926
HasMember	B	386	Symbolic Name not Mapping to Correct Object	1400	949
HasMember	C	400	Uncontrolled Resource Consumption	1400	971
HasMember	C	404	Improper Resource Shutdown or Release	1400	987
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	1400	993
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	1400	997
HasMember	C	407	Inefficient Algorithmic Complexity	1400	999
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	1400	1004
HasMember	B	410	Insufficient Resource Pool	1400	1005
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1400	1055
HasMember	V	453	Insecure Default Variable Initialization	1400	1091
HasMember	B	454	External Initialization of Trusted Variables or Data Stores	1400	1092

Nature	Type	ID	Name	V	Page
HasMember	V	456	Missing Initialization of a Variable	1400	1096
HasMember	V	457	Use of Uninitialized Variable	1400	1102
HasMember	B	459	Incomplete Cleanup	1400	1106
HasMember	B	460	Improper Cleanup on Thrown Exception	1400	1109
HasMember	B	471	Modification of Assumed-Immutable Data (MAID)	1400	1129
HasMember	B	487	Reliance on Package-level Scope	1400	1175
HasMember	V	495	Private Data Structure Returned From A Public Method	1400	1197
HasMember	V	496	Public Data Assigned to Private Array-Typed Field	1400	1199
HasMember	B	501	Trust Boundary Violation	1400	1210
HasMember	V	568	finalize() Method Without super.finalize()	1400	1299
HasMember	V	580	clone() Method Without super.clone()	1400	1319
HasMember	V	588	Attempt to Access Child of a Non-structure Pointer	1400	1332
HasMember	V	607	Public Static Final Field References Mutable Object	1400	1368
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1400	1373
HasMember	V	618	Exposed Unsafe ActiveX Method	1400	1389
HasMember	C	662	Improper Synchronization	1400	1457
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1400	1463
HasMember	C	665	Improper Initialization	1400	1465
HasMember	C	666	Operation on Resource in Wrong Phase of Lifetime	1400	1471
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1400	1480
HasMember	C	673	External Influence of Sphere Definition	1400	1492
HasMember	B	681	Incorrect Conversion between Numeric Types	1400	1504
HasMember	C	704	Incorrect Type Conversion or Cast	1400	1547
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	1400	1553
HasMember	B	749	Exposed Dangerous Method or Function	1400	1572
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1400	1622
HasMember	B	771	Missing Reference to Active Allocated Resource	1400	1631
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1400	1632
HasMember	V	773	Missing Reference to Active File Descriptor or Handle	1400	1638
HasMember	V	774	Allocation of File Descriptors or Handles Without Limits or Throttling	1400	1639
HasMember	V	775	Missing Release of File Descriptor or Handle after Effective Lifetime	1400	1640
HasMember	B	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	1400	1642
HasMember	B	779	Logging of Excessive Data	1400	1651
HasMember	V	782	Exposed IOCTL with Insufficient Access Control	1400	1657
HasMember	V	827	Improper Control of Document Type Definition	1400	1745
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1400	1750
HasMember	V	830	Inclusion of Web Functionality from an Untrusted Source	1400	1756
HasMember	B	843	Access of Resource Using Incompatible Type ('Type Confusion')	1400	1785
HasMember	B	908	Use of Uninitialized Resource	1400	1802
HasMember	C	909	Missing Initialization of Resource	1400	1806
HasMember	B	911	Improper Update of Reference Count	1400	1811
HasMember	C	913	Improper Control of Dynamically-Managed Code Resources	1400	1814
HasMember	B	920	Improper Restriction of Power Consumption	1400	1832

Nature	Type	ID	Name	V	Page
HasMember	C	922	Insecure Storage of Sensitive Information	1400	1835
HasMember	V	1042	Static Member Data Element outside of a Singleton Class Element	1400	1886
HasMember	B	1046	Creation of Immutable Text Using String Concatenation	1400	1890
HasMember	B	1049	Excessive Data Query Operations in a Large Data Table	1400	1894
HasMember	B	1050	Excessive Platform Resource Consumption within a Loop	1400	1895
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1400	1896
HasMember	B	1052	Excessive Use of Hard-Coded Literals in Initialization	1400	1897
HasMember	B	1063	Creation of Class Instance within a Static Code Block	1400	1910
HasMember	B	1067	Excessive Execution of Sequential Searches of Data Resource	1400	1914
HasMember	B	1072	Data Resource Access without Use of Connection Pooling	1400	1921
HasMember	B	1073	Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses	1400	1922
HasMember	B	1084	Invokable Control Element with Excessive File or Data Access Operations	1400	1933
HasMember	B	1089	Large Data Table with Excessive Number of Indices	1400	1938
HasMember	B	1091	Use of Object without Invoking Destructor Method	1400	1940
HasMember	B	1094	Excessive Index Range Scan for a Data Resource	1400	1943
HasMember	C	1176	Inefficient CPU Computation	1400	1980
HasMember	B	1188	Initialization of a Resource with an Insecure Default	1400	1983
HasMember	B	1221	Incorrect Register Defaults or Module Parameters	1400	2005
HasMember	C	1229	Creation of Emergent Resource	1400	2016
HasMember	B	1235	Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations	1400	2029
HasMember	V	1239	Improper Zeroization of Hardware Register	1400	2033
HasMember	B	1246	Improper Write Handling in Limited-write Non-Volatile Memories	1400	2054
HasMember	B	1250	Improper Preservation of Consistency Between Independent Representations of Shared State	1400	2064
HasMember	B	1258	Exposure of Sensitive System Information Due to Uncleared Debug Information	1400	2082
HasMember	B	1266	Improper Scrubbing of Sensitive Data from Decommissioned Device	1400	2104
HasMember	B	1271	Uninitialized Value on Reset for Registers Holding Security Settings	1400	2115
HasMember	B	1272	Sensitive Information Uncleared Before Debug/Power State Transition	1400	2116
HasMember	B	1279	Cryptographic Operations are run Before Supporting Units are Ready	1400	2132
HasMember	B	1301	Insufficient or Incomplete Data Removal within Hardware Component	1400	2183
HasMember	B	1325	Improperly Controlled Sequential Memory Allocation	1400	2222
HasMember	V	1330	Remanent Data Readable after Memory Erase	1400	2234
HasMember	B	1333	Inefficient Regular Expression Complexity	1400	2243
HasMember	B	1342	Information Exposure through Microarchitectural State after Transient Execution	1400	2262

Nature	Type	ID	Name	V	Page
HasMember	B	1386	Insecure Operation on Windows Junction / Mount Point	1400	2273
HasMember	B	1389	Incorrect Parsing of Numbers with Different Radices	1400	2275
HasMember	C	1419	Incorrect Initialization of Resource	1400	2292
HasMember	B	1420	Exposure of Sensitive Information during Transient Execution	1400	2297
HasMember	B	1421	Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution	1400	2304
HasMember	B	1422	Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution	1400	2310
HasMember	B	1423	Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution	1400	2316

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1417: Comprehensive Categorization: Sensitive Information Exposure

Category ID : 1417

Summary

Weaknesses in this category are related to sensitive information exposure.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	1400	511
HasMember	B	201	Insertion of Sensitive Information Into Sent Data	1400	521
HasMember	B	203	Observable Discrepancy	1400	525
HasMember	B	204	Observable Response Discrepancy	1400	530
HasMember	B	205	Observable Behavioral Discrepancy	1400	533
HasMember	V	206	Observable Internal Behavioral Discrepancy	1400	534
HasMember	V	207	Observable Behavioral Discrepancy With Equivalent Products	1400	535
HasMember	B	208	Observable Timing Discrepancy	1400	537
HasMember	B	209	Generation of Error Message Containing Sensitive Information	1400	540
HasMember	B	210	Self-generated Error Message Containing Sensitive Information	1400	546
HasMember	B	211	Externally-Generated Error Message Containing Sensitive Information	1400	548
HasMember	B	213	Exposure of Sensitive Information Due to Incompatible Policies	1400	555
HasMember	B	214	Invocation of Process Using Visible Sensitive Information	1400	556
HasMember	B	215	Insertion of Sensitive Information Into Debugging Code	1400	558

Nature	Type	ID	Name	V	Page
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	1400	889
HasMember	B	497	Exposure of Sensitive System Information to an Unauthorized Control Sphere	1400	1201
HasMember	V	526	Cleartext Storage of Sensitive Information in an Environment Variable	1400	1243
HasMember	V	531	Inclusion of Sensitive Information in Test Code	1400	1249
HasMember	B	532	Insertion of Sensitive Information into Log File	1400	1250
HasMember	V	535	Exposure of Information Through Shell Error Message	1400	1253
HasMember	V	536	Servlet Runtime Error Message Containing Sensitive Information	1400	1254
HasMember	V	537	Java Runtime Error Message Containing Sensitive Information	1400	1255
HasMember	B	538	Insertion of Sensitive Information into Externally-Accessible File or Directory	1400	1257
HasMember	B	540	Inclusion of Sensitive Information in Source Code	1400	1260
HasMember	V	541	Inclusion of Sensitive Information in an Include File	1400	1262
HasMember	V	548	Exposure of Information Through Directory Listing	1400	1269
HasMember	V	550	Server-generated Error Message Containing Sensitive Information	1400	1272
HasMember	V	598	Use of GET Request Method With Sensitive Query Strings	1400	1349
HasMember	V	615	Inclusion of Sensitive Information in Source Code Comments	1400	1383
HasMember	V	651	Exposure of WSDL File Containing Sensitive Information	1400	1442
HasMember	B	1254	Incorrect Comparison Logic Granularity	1400	2071
HasMember	V	1255	Comparison Logic is Vulnerable to Power Side-Channel Attacks	1400	2073
HasMember	B	1273	Device Unlock Credential Sharing	1400	2119
HasMember	B	1295	Debug Messages Revealing Unnecessary Information	1400	2164
HasMember	B	1300	Improper Protection of Physical Side Channels	1400	2177

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Category-1418: Comprehensive Categorization: Violation of Secure Design Principles

Category ID : 1418

Summary

Weaknesses in this category are related to violation of secure design principles.

Membership

Nature	Type	ID	Name	V	Page
MemberOf	V	1400	Comprehensive Categorization for Software Assurance Trends	1400	2619
HasMember	B	250	Execution with Unnecessary Privileges	1400	606

Nature	Type	ID	Name	V	Page
HasMember	C	424	Improper Protection of Alternate Path	1400	1031
HasMember	B	447	Unimplemented or Unsupported Feature in UI	1400	1082
HasMember	C	636	Not Failing Securely ('Failing Open')	1400	1409
HasMember	C	637	Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism')	1400	1411
HasMember	C	638	Not Using Complete Mediation	1400	1413
HasMember	C	653	Improper Isolation or Compartmentalization	1400	1445
HasMember	B	654	Reliance on a Single Factor in a Security Decision	1400	1448
HasMember	C	655	Insufficient Psychological Acceptability	1400	1450
HasMember	C	656	Reliance on Security Through Obscurity	1400	1452
HasMember	C	657	Violation of Secure Design Principles	1400	1454
HasMember	C	671	Lack of Administrator Control over Security	1400	1487
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1400	1985
HasMember	B	1192	Improper Identifier for IP Block used in System-On-Chip (SOC)	1400	1994
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1400	2186
HasMember	B	1331	Improper Isolation of Shared Resources in Network On Chip (NoC)	1400	2237
HasMember	C	1395	Dependency on Vulnerable Third-Party Component	1400	2289

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.2024-11-17.

Views

View-604: Deprecated Entries

View ID : 604
Type : Implicit

Objective

CWE nodes in this view (slice) have been deprecated. There should be a reference pointing to the replacement in each deprecated weakness.

Filter

/Weakness_Catalog/*/*[@Status='Deprecated']

Membership

Nature	Type	ID	Name	Page
HasMember	V	604	Deprecated Entries	2571

Metrics

	CWEs in this view
Weaknesses	25
Categories	35
Views	4
Total	64

View-629: Weaknesses in OWASP Top Ten (2007)

View ID : 629
Type : Graph

Objective

CWE nodes in this view (graph) are associated with the OWASP Top Ten, as released in 2007. This view is considered obsolete as a newer version of the OWASP Top Ten is available.

Audience

Software Developers

This view outlines the most important issues as identified by the OWASP Top Ten (2007 version), providing a good starting point for web application developers who want to code more securely.

Product Customers

This view outlines the most important issues as identified by the OWASP Top Ten (2007 version), providing customers with a way of asking their software developers to follow minimum expectations for secure code.

Educators

Since the OWASP Top Ten covers the most frequently encountered issues, this view can be used by educators as training material for students.

Membership

Nature	Type	ID	Name	Page
HasMember	C	712	OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)	2351
HasMember	C	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	2351
HasMember	C	714	OWASP Top Ten 2007 Category A3 - Malicious File Execution	2352
HasMember	C	715	OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference	2352
HasMember	C	716	OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF)	2353
HasMember	C	717	OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling	2353
HasMember	C	718	OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management	2353
HasMember	C	719	OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage	2354
HasMember	C	720	OWASP Top Ten 2007 Category A9 - Insecure Communications	2354
HasMember	C	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	2355

Notes

Relationship

The relationships in this view are a direct extraction of the CWE mappings that are in the 2007 OWASP document. CWE has changed since the release of that document.

References

[REF-43]OWASP. "OWASP TOP 10". 2007 May 8. < https://github.com/owasp-top/owasp-top-2007 >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	28	out of	940
Categories	10	out of	374
Views	0	out of	51
Total	38	out of	1365

View-635: Weaknesses Originally Used by NVD from 2008 to 2016

View ID : 635
Type : Explicit

Objective

CWE nodes in this view (slice) were used by NIST to categorize vulnerabilities within NVD, from 2008 to 2016. This original version has been used by many other projects.

Membership

Nature	Type	ID	Name	Page
HasMember	C	16	Configuration	2330
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	112
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	B	134	Use of Externally-Controlled Format String	371
HasMember	C	189	Numeric Errors	2333
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	511
HasMember	C	255	Credentials Management Errors	2336
HasMember	C	264	Permissions, Privileges, and Access Controls	2337
HasMember	C	287	Improper Authentication	699
HasMember	C	310	Cryptographic Issues	2339
HasMember	V	352	Cross-Site Request Forgery (CSRF)	875
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	895
HasMember	C	399	Resource Management Errors	2345

Notes

Maintenance

In Summer 2007, NIST began using this set of CWE elements to classify CVE entries within the National Vulnerability Database (NVD). The data was made publicly available beginning in 2008. In 2016, NIST began using a different list as derived from the "Weaknesses for Simplified Mapping of Published Vulnerabilities" view (CWE-1003).

References

[REF-1]NIST. "CWE - Common Weakness Enumeration". < http://nvd.nist.gov/cwe.cfm >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	13	out of	940
Categories	6	out of	374
Views	0	out of	51
Total	19	out of	1365

View-658: Weaknesses in Software Written in C

View ID : 658
Type : Implicit

Objective

This view (slice) covers issues that are found in C programs that are not common to all languages.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Applicable_Platforms/Language/@Name='C']

Membership

Nature	Type	ID	Name	Page
HasMember	V	658	Weaknesses in Software Written in C	2574

Metrics

	CWEs in this view		Total CWEs
Weaknesses	82	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	82	out of	1365

View-659: Weaknesses in Software Written in C++

View ID : 659
Type : Implicit

Objective

This view (slice) covers issues that are found in C++ programs that are not common to all languages.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Applicable_Platforms/Language/@Name='C++']

Membership

Nature	Type	ID	Name	Page
HasMember	V	659	Weaknesses in Software Written in C++	2574

Metrics

	CWEs in this view		Total CWEs
Weaknesses	86	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	86	out of	1365

View-660: Weaknesses in Software Written in Java

View ID : 660
Type : Implicit

Objective

This view (slice) covers issues that are found in Java programs that are not common to all languages.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Applicable_Platforms/Language/@Name='Java']

Membership

Nature	Type	ID	Name	Page
HasMember	V	660	Weaknesses in Software Written in Java	2575

Metrics

	CWEs in this view		Total CWEs
Weaknesses	77	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	77	out of	1365

View-661: Weaknesses in Software Written in PHP

View ID : 661
Type : Implicit

Objective

This view (slice) covers issues that are found in PHP programs that are not common to all languages.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Applicable_Platforms/Language/@Name='PHP']

Membership

Nature	Type	ID	Name	Page
HasMember	V	661	Weaknesses in Software Written in PHP	2575

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	25	out of	1365

View-677: Weakness Base Elements

View ID : 677
Type : Implicit

Objective

This view (slice) displays only weakness base elements.

Filter

/Weakness_Catalog/Weaknesses/Weakness[@Abstraction='Base'][not(@Status='Deprecated')]

Membership

Nature	Type	ID	Name	Page
HasMember	V	677	Weakness Base Elements	2575

Metrics

	CWEs in this view		Total CWEs
Weaknesses	521	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	521	out of	1365

View-678: Composites

View ID : 678
Type : Implicit

Objective

This view displays only composite weaknesses.

Filter

/Weakness_Catalog/Weaknesses/Weakness[@Structure='Composite'][not(@Status='Deprecated')]

Membership

Nature	Type	ID	Name	Page
HasMember	V	678	Composites	2576

Metrics

	CWEs in this view		Total CWEs
Weaknesses	4	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	4	out of	1365

View-699: Software Development

View ID : 699
Type : Graph

Objective

This view organizes weaknesses around concepts that are frequently used or encountered in software development. This includes all aspects of the software development lifecycle including both architecture and implementation. Accordingly, this view can align closely with the perspectives of architects, developers, educators, and assessment vendors. It provides a variety of categories that are intended to simplify navigation, browsing, and mapping.

Audience

Software Developers

Software developers (including architects, designers, coders, and testers) use this view to better understand potential mistakes that can be made in specific areas of their software application. The use of concepts that developers are familiar with makes it easier to navigate this view,

and filtering by Modes of Introduction can enable focus on a specific phase of the development lifecycle.

Educators

Educators use this view to teach future developers about the types of mistakes that are commonly made within specific parts of a codebase.

Membership

Nature	Type	ID	Name	Page
HasMember	C	19	Data Processing Errors	2330
HasMember	C	133	String Errors	2331
HasMember	C	136	Type Errors	2331
HasMember	C	137	Data Neutralization Issues	2332
HasMember	C	189	Numeric Errors	2333
HasMember	C	199	Information Management Errors	2333
HasMember	C	255	Credentials Management Errors	2336
HasMember	C	265	Privilege Issues	2338
HasMember	C	275	Permission Issues	2339
HasMember	C	310	Cryptographic Issues	2339
HasMember	C	320	Key Management Errors	2340
HasMember	C	355	User Interface Security Issues	2341
HasMember	C	371	State Issues	2342
HasMember	C	387	Signal Errors	2343
HasMember	C	389	Error Conditions, Return Values, Status Codes	2344
HasMember	C	399	Resource Management Errors	2345
HasMember	C	411	Resource Locking Problems	2346
HasMember	C	417	Communication Channel Errors	2347
HasMember	C	429	Handler Errors	2347
HasMember	C	438	Behavioral Problems	2348
HasMember	C	452	Initialization and Cleanup Errors	2348
HasMember	C	465	Pointer Issues	2349
HasMember	C	557	Concurrency Issues	2350
HasMember	C	569	Expression Issues	2351
HasMember	C	840	Business Logic Errors	2381
HasMember	C	1006	Bad Coding Practices	2443
HasMember	C	1210	Audit / Logging Errors	2496
HasMember	C	1211	Authentication Errors	2496
HasMember	C	1212	Authorization Errors	2497
HasMember	C	1213	Random Number Issues	2498
HasMember	C	1214	Data Integrity Issues	2498
HasMember	C	1215	Data Validation Issues	2499
HasMember	C	1216	Lockout Mechanism Errors	2499
HasMember	C	1217	User Session Errors	2500
HasMember	C	1218	Memory Buffer Errors	2500
HasMember	C	1219	File Handling Issues	2501
HasMember	C	1225	Documentation Issues	2501
HasMember	C	1226	Complexity Issues	2502
HasMember	C	1227	Encapsulation Issues	2502
HasMember	C	1228	API / Function Errors	2503

Notes

Other

The top level categories in this view represent commonly understood areas/terms within software development, and are meant to aid the user in identifying potential related weaknesses. It is possible for the same weakness to exist within multiple different categories.

Other

This view attempts to present weaknesses in a simple and intuitive way. As such it targets a single level of abstraction. It is important to realize that not every CWE will be represented in this view. High-level class weaknesses and low-level variant weaknesses are mostly ignored. However, by exploring the weaknesses that are included, and following the defined relationships, one can find these higher and lower level weaknesses.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	399	out of	940
Categories	40	out of	374
Views	0	out of	51
Total	439	out of	1365

View-700: Seven Pernicious Kingdoms

View ID : 700
Type : Graph

Objective

This view (graph) organizes weaknesses using a hierarchical structure that is similar to that used by Seven Pernicious Kingdoms.

Audience

Software Developers

This view is useful for developers because it is organized around concepts with which developers are familiar, and it focuses on weaknesses that can be detected using source code analysis tools.

Membership

Nature	Type	ID	Name	Page
HasMember	C	2	7PK - Environment	2329
HasMember	C	227	7PK - API Abuse	2334
HasMember	C	254	7PK - Security Features	2335
HasMember	C	361	7PK - Time and State	2341
HasMember	C	388	7PK - Errors	2343
HasMember	C	398	7PK - Code Quality	2344
HasMember	C	485	7PK - Encapsulation	2349
HasMember	C	1005	7PK - Input Validation and Representation	2442

Notes

Other

The MITRE CWE team frequently uses "7PK" as an abbreviation for Seven Pernicious Kingdoms.

References

[REF-6]Katrina Tsipenyuk, Brian Chess and Gary McGraw. "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors". NIST Workshop on Software Security Assurance Tools Techniques and Metrics. 2005 November 7. NIST. < https://samate.nist.gov/SSATTM_Content/

papers/Seven%20Pernicious%20Kingdoms%20-%20Taxonomy%20of%20Sw%20Security%20Errors%20-%20Tsipenyuk%20-%20Chess%20-%20McGraw.pdf >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	88	out of	940
Categories	9	out of	374
Views	0	out of	51
Total	97	out of	1365

View-701: Weaknesses Introduced During Design

View ID : 701
Type : Implicit

Objective

This view (slice) lists weaknesses that can be introduced during design.

Filter

/Weakness_Catalog/Weaknesses/Weakness[(@Abstraction='Base') or (@Abstraction='Class')][./Modes_Of_Introduction/Introduction/Phase='Architecture and Design']

Membership

Nature	Type	ID	Name	Page
HasMember	V	701	Weaknesses Introduced During Design	2579

Metrics

	CWEs in this view		Total CWEs
Weaknesses	274	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	274	out of	1365

View-702: Weaknesses Introduced During Implementation

View ID : 702
Type : Implicit

Objective

This view (slice) lists weaknesses that can be introduced during implementation.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Modes_Of_Introduction/Introduction/Phase='Implementation']

Membership

Nature	Type	ID	Name	Page
HasMember	V	702	Weaknesses Introduced During Implementation	2579

Metrics

	CWEs in this view		Total CWEs
Weaknesses	734	out of	940
Categories	0	out of	374
Views	0	out of	51

	CWEs in this view		Total CWEs
Total	734	out of	1365

View-709: Named Chains

View ID : 709
Type : Implicit

Objective

This view displays Named Chains and their components.

Filter

/Weakness_Catalog/Weaknesses/Weakness[@Structure='Chain']

Membership

Nature	Type	ID	Name	Page
HasMember	V	709	Named Chains	2580

Metrics

	CWEs in this view		Total CWEs
Weaknesses	3	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	3	out of	1365

View-711: Weaknesses in OWASP Top Ten (2004)

View ID : 711
Type : Graph

Objective

CWE entries in this view (graph) are associated with the OWASP Top Ten, as released in 2004, and as required for compliance with PCI DSS version 1.1. This view is considered obsolete as a newer version of the OWASP Top Ten is available.

Audience

Software Developers

This view outlines the most important issues as identified by the OWASP Top Ten (2004 version), providing a good starting point for web application developers who want to code more securely, as well as complying with PCI DSS 1.1.

Product Customers

This view outlines the most important issues as identified by the OWASP Top Ten, providing customers with a way of asking their software developers to follow minimum expectations for secure code, in compliance with PCI-DSS 1.1.

Educators

Since the OWASP Top Ten covers the most frequently encountered issues, this view can be used by educators as training material for students. However, the 2007 version (CWE-629) might be more appropriate.

Membership

Nature	Type	ID	Name	Page
HasMember	C	722	OWASP Top Ten 2004 Category A1 - Unvalidated Input	2355

Nature	Type	ID	Name	Page
HasMember	C	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	2356
HasMember	C	724	OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management	2356
HasMember	C	725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	2357
HasMember	C	726	OWASP Top Ten 2004 Category A5 - Buffer Overflows	2358
HasMember	C	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	2358
HasMember	C	728	OWASP Top Ten 2004 Category A7 - Improper Error Handling	2359
HasMember	C	729	OWASP Top Ten 2004 Category A8 - Insecure Storage	2359
HasMember	C	730	OWASP Top Ten 2004 Category A9 - Denial of Service	2360
HasMember	C	731	OWASP Top Ten 2004 Category A10 - Insecure Configuration Management	2360

Notes

Relationship

CWE relationships for this view were obtained by examining the OWASP document and mapping to any items that were specifically mentioned within the text of a category. As a result, this mapping is not complete with respect to all of CWE. In addition, some concepts were mentioned in multiple Top Ten items, which caused them to be mapped to multiple CWE categories. For example, SQL injection is mentioned in both A1 (CWE-722) and A6 (CWE-727) categories.

Relationship

As of 2008, some parts of CWE were not fully clarified out in terms of weaknesses. When these areas were mentioned in the OWASP Top Ten, category entries were mapped, although general mapping practice would usually favor mapping only to weaknesses.

References

[REF-570]"Top 10 2004". 2004 January 7. OWASP. < http://www.owasp.org/index.php/Top_10_2004 >.
[REF-571]PCI Security Standards Council. "About the PCI Data Security Standard (PCI DSS)". < https://listings.pcisecuritystandards.org/pci_security/ >.2023-04-07.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	117	out of	940
Categories	13	out of	374
Views	0	out of	51
Total	130	out of	1365

View-734: Weaknesses Addressed by the CERT C Secure Coding Standard (2008)

View ID : 734
Type : Graph

Objective

CWE entries in this view (graph) are fully or partially eliminated by following the guidance presented in the book "The CERT C Secure Coding Standard" published in 2008. This view is considered obsolete, as a newer version of the coding standard is available. This view statically represents the coding rules as they were in 2008.

Audience

Software Developers

By following the CERT C Secure Coding Standard, developers will be able to fully or partially prevent the weaknesses that are identified in this view. In addition, developers can use a CWE coverage graph to determine which weaknesses are not directly addressed by the standard, which will help identify and resolve remaining gaps in training, tool acquisition, or other approaches for reducing weaknesses.

Product Customers

If a software developer claims to be following the CERT C Secure Coding standard, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could link them to the relevant Secure Coding Standard.

Membership

Nature	Type	ID	Name	Page
HasMember	C	735	CERT C Secure Coding Standard (2008) Chapter 2 - Preprocessor (PRE)	2361
HasMember	C	736	CERT C Secure Coding Standard (2008) Chapter 3 - Declarations and Initialization (DCL)	2362
HasMember	C	737	CERT C Secure Coding Standard (2008) Chapter 4 - Expressions (EXP)	2362
HasMember	C	738	CERT C Secure Coding Standard (2008) Chapter 5 - Integers (INT)	2363
HasMember	C	739	CERT C Secure Coding Standard (2008) Chapter 6 - Floating Point (FLP)	2364
HasMember	C	740	CERT C Secure Coding Standard (2008) Chapter 7 - Arrays (ARR)	2365
HasMember	C	741	CERT C Secure Coding Standard (2008) Chapter 8 - Characters and Strings (STR)	2366
HasMember	C	742	CERT C Secure Coding Standard (2008) Chapter 9 - Memory Management (MEM)	2367
HasMember	C	743	CERT C Secure Coding Standard (2008) Chapter 10 - Input Output (FIO)	2368
HasMember	C	744	CERT C Secure Coding Standard (2008) Chapter 11 - Environment (ENV)	2369
HasMember	C	745	CERT C Secure Coding Standard (2008) Chapter 12 - Signals (SIG)	2370
HasMember	C	746	CERT C Secure Coding Standard (2008) Chapter 13 - Error Handling (ERR)	2371
HasMember	C	747	CERT C Secure Coding Standard (2008) Chapter 14 - Miscellaneous (MSC)	2371
HasMember	C	748	CERT C Secure Coding Standard (2008) Appendix - POSIX (POS)	2372

Notes

Relationship

The relationships in this view were determined based on specific statements within the rules from the standard. Not all rules have direct relationships to individual weaknesses, although they likely have chaining relationships in specific circumstances.

References

[REF-597]Robert C. Seacord. "The CERT C Secure Coding Standard". 1st Edition. 2008 October 4. Addison-Wesley Professional.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	91	out of	940
Categories	14	out of	374
Views	0	out of	51
Total	105	out of	1365

View-750: Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors

View ID : 750
Type : Graph

Objective

CWE entries in this view (graph) are listed in the 2009 CWE/SANS Top 25 Programming Errors. This view is considered obsolete as a newer version of the Top 25 is available.

Audience

Software Developers

By following the Top 25, developers will be able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

If a software developer claims to be following the Top 25, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could focus on the Top 25.

Membership

Nature	Type	ID	Name	Page
HasMember	C	751	2009 Top 25 - Insecure Interaction Between Components	2373
HasMember	C	752	2009 Top 25 - Risky Resource Management	2374
HasMember	C	753	2009 Top 25 - Porous Defenses	2374

References

[REF-615]"2009 CWE/SANS Top 25 Most Dangerous Programming Errors". 2009 January 2. < https://cwe.mitre.org/top25/archive/2009/2009_cwe_sans_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	26	out of	940
Categories	3	out of	374
Views	0	out of	51
Total	29	out of	1365

View-800: Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors

View ID : 800
Type : Graph

Objective

CWE entries in this view (graph) are listed in the 2010 CWE/SANS Top 25 Programming Errors. This view is considered obsolete as a newer version of the Top 25 is available.

Audience

Software Developers

By following the Top 25, developers will be able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

If a software developer claims to be following the Top 25, then customers can use the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could focus on the Top 25.

Membership

Nature	Type	ID	Name	Page
HasMember	C	801	2010 Top 25 - Insecure Interaction Between Components	2375
HasMember	C	802	2010 Top 25 - Risky Resource Management	2375
HasMember	C	803	2010 Top 25 - Porous Defenses	2376
HasMember	C	808	2010 Top 25 - Weaknesses On the Cusp	2376

References

[REF-732]"2010 CWE/SANS Top 25 Most Dangerous Software Errors". 2010 February 4. < https://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	41	out of	940
Categories	4	out of	374
Views	0	out of	51
Total	45	out of	1365

View-809: Weaknesses in OWASP Top Ten (2010)

View ID : 809
Type : Graph

Objective

CWE nodes in this view (graph) are associated with the OWASP Top Ten, as released in 2010. This view is considered obsolete as a newer version of the OWASP Top Ten is available.

Audience

Software Developers

This view outlines the most important issues as identified by the OWASP Top Ten (2010 version), providing a good starting point for web application developers who want to code more securely.

Product Customers

This view outlines the most important issues as identified by the OWASP Top Ten (2010 version), providing customers with a way of asking their software developers to follow minimum expectations for secure code.

Educators

Since the OWASP Top Ten covers the most frequently encountered issues, this view can be used by educators as training material for students.

Membership

Nature	Type	ID	Name	Page
HasMember	C	810	OWASP Top Ten 2010 Category A1 - Injection	2377
HasMember	C	811	OWASP Top Ten 2010 Category A2 - Cross-Site Scripting (XSS)	2378
HasMember	C	812	OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management	2378
HasMember	C	813	OWASP Top Ten 2010 Category A4 - Insecure Direct Object References	2378
HasMember	C	814	OWASP Top Ten 2010 Category A5 - Cross-Site Request Forgery(CSRF)	2379
HasMember	C	815	OWASP Top Ten 2010 Category A6 - Security Misconfiguration	2379
HasMember	C	816	OWASP Top Ten 2010 Category A7 - Insecure Cryptographic Storage	2380
HasMember	C	817	OWASP Top Ten 2010 Category A8 - Failure to Restrict URL Access	2380
HasMember	C	818	OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection	2381
HasMember	C	819	OWASP Top Ten 2010 Category A10 - Unvalidated Redirects and Forwards	2381

Notes

Relationship

The relationships in this view are a direct extraction of the CWE mappings that are in the 2010 OWASP document. CWE has changed since the release of that document.

References

[REF-759]"Top 10 2010". 2010 April 9. OWASP. < https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2010 >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	32	out of	940
Categories	10	out of	374
Views	0	out of	51
Total	42	out of	1365

View-844: Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)

View ID : 844
Type : Graph

Objective

CWE entries in this view (graph) are fully or partially eliminated by following the guidance presented in the book "The CERT Oracle Secure Coding Standard for Java" published in 2011. This view is considered obsolete as a newer version of the coding standard is available.

Audience

Software Developers

By following The CERT Oracle Secure Coding Standard for Java, developers will be able to fully or partially prevent the weaknesses that are identified in this view. In addition, developers can use a CWE coverage graph to determine which weaknesses are not directly addressed by the standard, which will help identify and resolve remaining gaps in training, tool acquisition, or other approaches for reducing weaknesses.

Product Customers

If a software developer claims to be following The CERT Oracle Secure Coding Standard for Java, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could link them to the relevant Secure Coding Standard.

Membership

Nature	Type	ID	Name	Page
HasMember	C	845	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 2 - Input Validation and Data Sanitization (IDS)	2383
HasMember	C	846	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 3 - Declarations and Initialization (DCL)	2383
HasMember	C	847	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 4 - Expressions (EXP)	2384
HasMember	C	848	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 5 - Numeric Types and Operations (NUM)	2384
HasMember	C	849	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 6 - Object Orientation (OBJ)	2385
HasMember	C	850	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 7 - Methods (MET)	2385
HasMember	C	851	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 8 - Exceptional Behavior (ERR)	2386
HasMember	C	852	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 9 - Visibility and Atomicity (VNA)	2387
HasMember	C	853	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 10 - Locking (LCK)	2387
HasMember	C	854	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 11 - Thread APIs (THI)	2388
HasMember	C	855	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 12 - Thread Pools (TPS)	2388
HasMember	C	856	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 13 - Thread-Safety Miscellaneous (TSM)	2389
HasMember	C	857	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 14 - Input Output (FIO)	2389
HasMember	C	858	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 15 - Serialization (SER)	2390
HasMember	C	859	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 16 - Platform Security (SEC)	2390
HasMember	C	860	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 17 - Runtime Environment (ENV)	2391

Nature	Type	ID	Name	Page
HasMember	C	861	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 18 - Miscellaneous (MSC)	2391

Notes

Relationship

The relationships in this view were determined based on specific statements within the rules from the standard. Not all rules have direct relationships to individual weaknesses, although they likely have chaining relationships in specific circumstances.

References

[REF-813]Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland and David Svoboda. "The CERT Oracle Coding Standard for Java". 1st Edition. 2011 September 8. Addison-Wesley Professional.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	104	out of	940
Categories	17	out of	374
Views	0	out of	51
Total	121	out of	1365

View-868: Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)

View ID : 868
Type : Graph

Objective

CWE entries in this view (graph) are fully or partially eliminated by following the SEI CERT C++ Coding Standard, as published in 2016. This view is no longer being actively maintained, since it statically represents the coding rules as they were in 2016.

Audience

Software Developers

By following the CERT C++ Secure Coding Standard, developers will be able to fully or partially prevent the weaknesses that are identified in this view. In addition, developers can use a CWE coverage graph to determine which weaknesses are not directly addressed by the standard, which will help identify and resolve remaining gaps in training, tool acquisition, or other approaches for reducing weaknesses.

Product Customers

If a software developer claims to be following the CERT C++ Secure Coding Standard, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could link them to the relevant Secure Coding Standard.

Membership

Nature	Type	ID	Name	Page
HasMember	C	869	CERT C++ Secure Coding Section 01 - Preprocessor (PRE)	2394

Nature	Type	ID	Name	Page
HasMember	C	870	CERT C++ Secure Coding Section 02 - Declarations and Initialization (DCL)	2395
HasMember	C	871	CERT C++ Secure Coding Section 03 - Expressions (EXP)	2395
HasMember	C	872	CERT C++ Secure Coding Section 04 - Integers (INT)	2395
HasMember	C	873	CERT C++ Secure Coding Section 05 - Floating Point Arithmetic (FLP)	2396
HasMember	C	874	CERT C++ Secure Coding Section 06 - Arrays and the STL (ARR)	2396
HasMember	C	875	CERT C++ Secure Coding Section 07 - Characters and Strings (STR)	2397
HasMember	C	876	CERT C++ Secure Coding Section 08 - Memory Management (MEM)	2398
HasMember	C	877	CERT C++ Secure Coding Section 09 - Input Output (FIO)	2398
HasMember	C	878	CERT C++ Secure Coding Section 10 - Environment (ENV)	2399
HasMember	C	879	CERT C++ Secure Coding Section 11 - Signals (SIG)	2400
HasMember	C	880	CERT C++ Secure Coding Section 12 - Exceptions and Error Handling (ERR)	2400
HasMember	C	881	CERT C++ Secure Coding Section 13 - Object Oriented Programming (OOP)	2401
HasMember	C	882	CERT C++ Secure Coding Section 14 - Concurrency (CON)	2401
HasMember	C	883	CERT C++ Secure Coding Section 49 - Miscellaneous (MSC)	2402

Notes

Relationship

The relationships in this view were determined based on specific statements within the rules from the standard. Not all rules have direct relationships to individual weaknesses, although they likely have chaining relationships in specific circumstances.

References

[REF-847]The Software Engineering Institute. "SEI CERT C++ Coding Standard". < https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682 >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	95	out of	940
Categories	15	out of	374
Views	0	out of	51
Total	110	out of	1365

View-884: CWE Cross-section

View ID : 884
Type : Explicit

Objective

This view contains a selection of weaknesses that represent the variety of weaknesses that are captured in CWE, at a level of abstraction that is likely to be useful to most audiences. It can be used by researchers to determine how broad their theories, models, or tools are. It will also be used by the CWE content team in 2012 to focus quality improvement efforts for individual CWE entries.

Membership

Nature	Type	ID	Name	Page
HasMember	V	14	Compiler Removal of Code to Clear Buffers	14
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	B	23	Relative Path Traversal	46
HasMember	B	36	Absolute Path Traversal	75
HasMember	B	41	Improper Resolution of Path Equivalence	87
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	112
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	198
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	217
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	232
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	238
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	249
HasMember	V	113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')	277
HasMember	B	117	Improper Output Neutralization for Logs	294
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	310
HasMember	V	129	Improper Validation of Array Index	347
HasMember	B	131	Incorrect Calculation of Buffer Size	361
HasMember	B	134	Use of Externally-Controlled Format String	371
HasMember	B	135	Incorrect Calculation of Multi-Byte String Length	377
HasMember	B	170	Improper Null Termination	434
HasMember	V	173	Improper Handling of Alternate Encoding	441
HasMember	V	174	Double Decoding of the Same Data	443
HasMember	V	175	Improper Handling of Mixed Encoding	445
HasMember	B	179	Incorrect Behavior Order: Early Validation	454
HasMember	C	185	Incorrect Regular Expression	469
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	487
HasMember	B	193	Off-by-one Error	493
HasMember	B	203	Observable Discrepancy	525
HasMember	B	209	Generation of Error Message Containing Sensitive Information	540
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	551
HasMember	B	222	Truncation of Security-relevant Information	565
HasMember	B	223	Omission of Security-relevant Information	566
HasMember	C	228	Improper Handling of Syntactically Invalid Structure	575

Nature	Type	ID	Name	Page
HasMember	V	244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	598
HasMember	B	248	Uncaught Exception	603
HasMember	B	250	Execution with Unnecessary Privileges	606
HasMember	B	252	Unchecked Return Value	613
HasMember	B	253	Incorrect Check of Function Return Value	620
HasMember	B	262	Not Using Password Aging	640
HasMember	B	263	Password Aging with Long Expiration	643
HasMember	B	266	Incorrect Privilege Assignment	645
HasMember	B	267	Privilege Defined With Unsafe Actions	648
HasMember	B	268	Privilege Chaining	651
HasMember	B	270	Privilege Context Switching Error	659
HasMember	C	271	Privilege Dropping / Lowering Errors	660
HasMember	B	273	Improper Check for Dropped Privileges	667
HasMember	B	283	Unverified Ownership	685
HasMember	B	290	Authentication Bypass by Spoofing	712
HasMember	B	294	Authentication Bypass by Capture-replay	719
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	726
HasMember	B	299	Improper Check for Certificate Revocation	734
HasMember	C	300	Channel Accessible by Non-Endpoint	737
HasMember	B	301	Reflection Attack in an Authentication Protocol	740
HasMember	B	304	Missing Critical Step in Authentication	745
HasMember	B	306	Missing Authentication for Critical Function	748
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	754
HasMember	B	308	Use of Single-factor Authentication	759
HasMember	B	312	Cleartext Storage of Sensitive Information	771
HasMember	B	319	Cleartext Transmission of Sensitive Information	786
HasMember	B	322	Key Exchange without Entity Authentication	795
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	797
HasMember	B	325	Missing Cryptographic Step	801
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	806
HasMember	B	331	Insufficient Entropy	828
HasMember	B	334	Small Space of Random Values	834
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	836
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	844
HasMember	B	341	Predictable from Observable State	850
HasMember	B	347	Improper Verification of Cryptographic Signature	864
HasMember	B	348	Use of Less Trusted Source	866
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	868
HasMember	F	352	Cross-Site Request Forgery (CSRF)	875
HasMember	B	353	Missing Support for Integrity Check	881
HasMember	B	354	Improper Validation of Integrity Check Value	883
HasMember	B	364	Signal Handler Race Condition	905
HasMember	B	367	Time-of-check Time-of-use (TOCTOU) Race Condition	913
HasMember	B	369	Divide By Zero	920
HasMember	B	390	Detection of Error Condition Without Action	950

Nature	Type	ID	Name	Page
HasMember	B	392	Missing Report of Error Condition	958
HasMember	B	393	Return of Wrong Status Code	960
HasMember	C	400	Uncontrolled Resource Consumption	971
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	997
HasMember	C	407	Inefficient Algorithmic Complexity	999
HasMember	B	408	Incorrect Behavior Order: Early Amplification	1002
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	1004
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	1075
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1087
HasMember	V	453	Insecure Default Variable Initialization	1091
HasMember	B	454	External Initialization of Trusted Variables or Data Stores	1092
HasMember	B	455	Non-exit on Failed Initialization	1095
HasMember	V	456	Missing Initialization of a Variable	1096
HasMember	V	467	Use of sizeof() on a Pointer Type	1118
HasMember	B	468	Incorrect Pointer Scaling	1121
HasMember	B	469	Use of Pointer Subtraction to Determine Size	1123
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1125
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	478	Missing Default Case in Multiple Condition Expression	1149
HasMember	B	480	Use of Incorrect Operator	1157
HasMember	B	483	Incorrect Block Delimitation	1167
HasMember	B	484	Omitted Break Statement in Switch	1169
HasMember	V	486	Comparison of Classes by Name	1172
HasMember	B	494	Download of Code Without Integrity Check	1192
HasMember	V	495	Private Data Structure Returned From A Public Method	1197
HasMember	V	496	Public Data Assigned to Private Array-Typed Field	1199
HasMember	V	498	Cloneable Class Containing Sensitive Information	1204
HasMember	V	499	Serializable Class Containing Sensitive Data	1206
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	B	521	Weak Password Requirements	1231
HasMember	C	522	Insufficiently Protected Credentials	1234
HasMember	V	546	Suspicious Comment	1266
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	1267
HasMember	B	561	Dead Code	1283
HasMember	B	563	Assignment to Variable without Use	1289
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	1296
HasMember	V	587	Assignment of a Fixed Address to a Pointer	1330
HasMember	V	595	Comparison of Object References Instead of Object Contents	1342
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1353
HasMember	C	602	Client-Side Enforcement of Server-Side Security	1359
HasMember	V	605	Multiple Binds to the Same Port	1364
HasMember	B	617	Reachable Assertion	1387
HasMember	V	621	Variable Extraction Error	1394

Nature	Type	ID	Name	Page
HasMember	V	627	Dynamic Variable Evaluation	1405
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1407
HasMember	C	642	External Control of Critical State Data	1422
HasMember	B	648	Incorrect Use of Privileged APIs	1437
HasMember	C	667	Improper Locking	1472
HasMember	C	672	Operation on a Resource after Expiration or Release	1488
HasMember	C	674	Uncontrolled Recursion	1493
HasMember	B	676	Use of Potentially Dangerous Function	1498
HasMember	B	681	Incorrect Conversion between Numeric Types	1504
HasMember	B	698	Execution After Redirect (EAR)	1542
HasMember	B	708	Incorrect Ownership Assignment	1556
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1559
HasMember	B	756	Missing Custom Error Page	1588
HasMember	B	763	Release of Invalid Pointer or Reference	1608
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1622
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1632
HasMember	B	783	Operator Precedence Logic Error	1659
HasMember	B	786	Access of Memory Location Before Start of Buffer	1666
HasMember	B	788	Access of Memory Location After End of Buffer	1678
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	B	805	Buffer Access with Incorrect Length Value	1711
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1723
HasMember	B	822	Untrusted Pointer Dereference	1732
HasMember	B	825	Expired Pointer Dereference	1741
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1750
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1766
HasMember	B	838	Inappropriate Encoding for Output Context	1773
HasMember	B	839	Numeric Range Comparison Without Minimum Check	1776
HasMember	B	841	Improper Enforcement of Behavioral Workflow	1781
HasMember	C	862	Missing Authorization	1789
HasMember	C	863	Incorrect Authorization	1796

Metrics

	CWEs in this view		Total CWEs
Weaknesses	157	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	157	out of	1365

View-888: Software Fault Pattern (SFP) Clusters

View ID : 888
Type : Graph

Objective

CWE identifiers in this view are associated with clusters of Software Fault Patterns (SFPs).

Audience

Applied Researchers

Academic Researchers

Product Vendors

Membership

Nature	Type	ID	Name	Page
HasMember	C	885	SFP Primary Cluster: Risky Values	2403
HasMember	C	886	SFP Primary Cluster: Unused entities	2403
HasMember	C	887	SFP Primary Cluster: API	2403
HasMember	C	889	SFP Primary Cluster: Exception Management	2403
HasMember	C	890	SFP Primary Cluster: Memory Access	2404
HasMember	C	891	SFP Primary Cluster: Memory Management	2404
HasMember	C	892	SFP Primary Cluster: Resource Management	2404
HasMember	C	893	SFP Primary Cluster: Path Resolution	2405
HasMember	C	894	SFP Primary Cluster: Synchronization	2405
HasMember	C	895	SFP Primary Cluster: Information Leak	2405
HasMember	C	896	SFP Primary Cluster: Tainted Input	2406
HasMember	C	897	SFP Primary Cluster: Entry Points	2406
HasMember	C	898	SFP Primary Cluster: Authentication	2406
HasMember	C	899	SFP Primary Cluster: Access Control	2407
HasMember	C	901	SFP Primary Cluster: Privilege	2407
HasMember	C	902	SFP Primary Cluster: Channel	2408
HasMember	C	903	SFP Primary Cluster: Cryptography	2408
HasMember	C	904	SFP Primary Cluster: Malware	2408
HasMember	C	905	SFP Primary Cluster: Predictability	2409
HasMember	C	906	SFP Primary Cluster: UI	2409
HasMember	C	907	SFP Primary Cluster: Other	2409
HasMember	C	1237	SFP Primary Cluster: Faulty Resource Release	2503
HasMember	C	1238	SFP Primary Cluster: Failure to Release Memory	2503

References

[REF-19]Nikolai Mansourov and Djenana Campara. "System Assurance". 2010 December 6. < https://www.elsevier.com/books/system-assurance/mansourov/978-0-12-381414-2 >.
[REF-20]Ben Calloni, Nikolai Mansourov and Djenana Campara. "Task Order 0006: Vulnerability Path Analysis and Demonstration (VPAD). Volume 2 - White Box Definitions of Software Fault Patterns". 2011 December. < https://apps.dtic.mil/docs/citations/ADB381215 >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	614	out of	940
Categories	83	out of	374
Views	0	out of	51
Total	697	out of	1365

View-900: Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors

View ID : 900
Type : Graph

Objective

CWE entries in this view (graph) are listed in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors.

Audience

Software Developers

By following the Top 25, developers will be able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

If a software developer claims to be following the Top 25, then customers can use the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could focus on the Top 25.

Membership

Nature	Type	ID	Name	Page
HasMember	C	864	2011 Top 25 - Insecure Interaction Between Components	2392
HasMember	C	865	2011 Top 25 - Risky Resource Management	2392
HasMember	C	866	2011 Top 25 - Porous Defenses	2393
HasMember	C	867	2011 Top 25 - Weaknesses On the Cusp	2393

References

[REF-843]"2011 CWE/SANS Top 25 Most Dangerous Software Errors". 2011 June 7. < https://cwe.mitre.org/top25/archive/2011/2011_cwe_sans_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	41	out of	940
Categories	4	out of	374
Views	0	out of	51
Total	45	out of	1365

View-919: Weaknesses in Mobile Applications

View ID : 919
Type : Implicit

Objective

CWE entries in this view (slice) are often seen in mobile applications.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Applicable_Platforms/Technology/@Class='Mobile']

Membership

Nature	Type	ID	Name	Page
HasMember	V	919	Weaknesses in Mobile Applications	2594

Metrics

	CWEs in this view		Total CWEs
Weaknesses	21	out of	940
Categories	0	out of	374
Views	0	out of	51

	CWEs in this view		Total CWEs
Total	21	out of	1365

View-928: Weaknesses in OWASP Top Ten (2013)

View ID : 928
Type : Graph

Objective

CWE nodes in this view (graph) are associated with the OWASP Top Ten, as released in 2013. This view is considered obsolete as a newer version of the OWASP Top Ten is available.

Audience

Software Developers

This view outlines the most important issues as identified by the OWASP Top Ten (2013 version), providing a good starting point for web application developers who want to code more securely.

Product Customers

This view outlines the most important issues as identified by the OWASP Top Ten (2013 version), providing customers with a way of asking their software developers to follow minimum expectations for secure code.

Educators

Since the OWASP Top Ten covers the most frequently encountered issues, this view can be used by educators as training material for students.

Membership

Nature	Type	ID	Name	Page
HasMember	C	929	OWASP Top Ten 2013 Category A1 - Injection	2410
HasMember	C	930	OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management	2410
HasMember	C	931	OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS)	2411
HasMember	C	932	OWASP Top Ten 2013 Category A4 - Insecure Direct Object References	2411
HasMember	C	933	OWASP Top Ten 2013 Category A5 - Security Misconfiguration	2412
HasMember	C	934	OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure	2412
HasMember	C	935	OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control	2413
HasMember	C	936	OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF)	2413
HasMember	C	937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities	2413
HasMember	C	938	OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards	2414

Notes

Relationship

The relationships in this view have been pulled directly from the 2013 OWASP Top 10 document, either from the explicit mapping section, or from weakness types alluded to in the written sections.

References

[REF-926]"Top 10 2013". 2013 June 2. OWASP. < https://www.owasp.org/index.php/Top_10_2013 >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	36	out of	940
Categories	13	out of	374
Views	0	out of	51
Total	49	out of	1365

View-1000: Research Concepts

View ID : 1000
Type : Graph

Objective

This view is intended to facilitate research into weaknesses, including their inter-dependencies, and can be leveraged to systematically identify theoretical gaps within CWE. It is mainly organized according to abstractions of behaviors instead of how they can be detected, where they appear in code, or when they are introduced in the development life cycle. By design, this view is expected to include every weakness within CWE.

Audience

Academic Researchers

Academic researchers can use the high-level classes that lack a significant number of children to identify potential areas for future research.

Vulnerability Analysts

Those who perform vulnerability discovery/analysis use this view to identify related weaknesses that might be leveraged by following relationships between higher-level classes and bases.

Assessment Tool Vendors

Assessment vendors often use this view to help identify additional weaknesses that a tool may be able to detect as the relationships are more aligned with a tool's technical capabilities.

Membership

Nature	Type	ID	Name	Page
HasMember	P	284	Improper Access Control	687
HasMember	P	435	Improper Interaction Between Multiple Correctly-Behaving Entities	1063
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1463
HasMember	P	682	Incorrect Calculation	1507
HasMember	P	691	Insufficient Control Flow Management	1525
HasMember	P	693	Protection Mechanism Failure	1529
HasMember	P	697	Incorrect Comparison	1538
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1544
HasMember	P	707	Improper Neutralization	1554
HasMember	P	710	Improper Adherence to Coding Standards	1558

Notes

Other

This view uses a deep hierarchical organization, with more levels of abstraction than other classification schemes. The top-level entries are called Pillars. Where possible, this view uses abstractions that do not consider particular languages, frameworks, technologies, life cycle development phases, frequency of occurrence, or types of resources. It explicitly identifies relationships that form chains and composites, which have not been a formal part of past classification efforts. Chains and composites might help explain why mutual exclusivity is difficult to achieve within security error taxonomies. This view is roughly aligned with MITRE's research into vulnerability theory, especially with respect to behaviors and resources. Ideally, this view will only cover weakness-to-weakness relationships, with minimal overlap and zero categories. It is expected to include at least one parent/child relationship for every weakness within CWE.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	940	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	940	out of	1365

View-1003: Weaknesses for Simplified Mapping of Published Vulnerabilities

View ID : 1003
Type : Graph

Objective

CWE entries in this view (graph) may be used to categorize potential weaknesses within sources that handle public, third-party vulnerability information, such as the National Vulnerability Database (NVD). By design, this view is incomplete. It is limited to a small number of the most commonly-seen weaknesses, so that it is easier for humans to use. This view uses a shallow hierarchy of two levels in order to simplify the complex navigation of the entire CWE corpus.

Membership

Nature	Type	ID	Name	Page
HasMember		20	Improper Input Validation	20
HasMember		74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	138
HasMember		116	Improper Encoding or Escaping of Output	287
HasMember		119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember		200	Exposure of Sensitive Information to an Unauthorized Actor	511
HasMember		269	Improper Privilege Management	653
HasMember		287	Improper Authentication	699
HasMember		311	Missing Encryption of Sensitive Data	764
HasMember		326	Inadequate Encryption Strength	803
HasMember		327	Use of a Broken or Risky Cryptographic Algorithm	806
HasMember		330	Use of Insufficiently Random Values	821
HasMember		345	Insufficient Verification of Data Authenticity	858
HasMember		362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	895
HasMember		400	Uncontrolled Resource Consumption	971
HasMember		404	Improper Resource Shutdown or Release	987
HasMember		407	Inefficient Algorithmic Complexity	999
HasMember		436	Interpretation Conflict	1065

Nature	Type	ID	Name	Page
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1373
HasMember	C	662	Improper Synchronization	1457
HasMember	C	665	Improper Initialization	1465
HasMember	C	668	Exposure of Resource to Wrong Sphere	1478
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1480
HasMember	C	670	Always-Incorrect Control Flow Implementation	1484
HasMember	C	672	Operation on a Resource after Expiration or Release	1488
HasMember	C	674	Uncontrolled Recursion	1493
HasMember	P	682	Incorrect Calculation	1507
HasMember	P	697	Incorrect Comparison	1538
HasMember	C	704	Incorrect Type Conversion or Cast	1547
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	1553
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1559
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1577
HasMember	C	755	Improper Handling of Exceptional Conditions	1585
HasMember	C	834	Excessive Iteration	1763
HasMember	C	862	Missing Authorization	1789
HasMember	C	863	Incorrect Authorization	1796
HasMember	C	913	Improper Control of Dynamically-Managed Code Resources	1814
HasMember	C	922	Insecure Storage of Sensitive Information	1835

Notes

Maintenance

This view may change in any upcoming CWE version based on the experience of NVD analysts, public feedback, and the CWE Team - especially with respect to the CWE Top 25 analysis.

Maintenance

This view has been modified significantly since its last major revision in 2016 (CWE-635 was used before 2016).

References

[REF-1]NIST. "CWE - Common Weakness Enumeration". < http://nvd.nist.gov/cwe.cfm >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	130	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	130	out of	1365

View-1008: Architectural Concepts

View ID : 1008
Type : Graph

Objective

This view organizes weaknesses according to common architectural security tactics. It is intended to assist architects in identifying potential mistakes that can be made when designing software.

Audience

Software Developers

Architects that are part of a software development team may find this view useful as the weaknesses are organized by known security tactics, aiding the arcitect in embedding security throughout the design process instead of discovering weaknesses after the software has been built.

Educators

Educators may use this view as reference material when discussing security by design or architectural weaknesses, and the types of mistakes that can be made.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1009	Audit	2445
HasMember	C	1010	Authenticate Actors	2445
HasMember	C	1011	Authorize Actors	2446
HasMember	C	1012	Cross Cutting	2448
HasMember	C	1013	Encrypt Data	2449
HasMember	C	1014	Identify Actors	2450
HasMember	C	1015	Limit Access	2451
HasMember	C	1016	Limit Exposure	2452
HasMember	C	1017	Lock Computer	2452
HasMember	C	1018	Manage User Sessions	2453
HasMember	C	1019	Validate Inputs	2454
HasMember	C	1020	Verify Message Integrity	2455

Notes

Other

The top level categories in this view represent the individual tactics that are part of a secure-by-design approach to software development. The weaknesses that are members of each category contain information about how each is introduced relative to the software's architecture. Three different modes of introduction are used: Omission - caused by missing a security tactic when it is necessary. Commission - refers to incorrect choice of tactics which could result in undesirable consequences. Realization - appropriate security tactics are adopted but are incorrectly implemented.

References

[REF-9]Santos, J. C. S., Tarrit, K. and Mirakhorli, M.. "A Catalog of Security Architecture Weaknesses.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/cawe-paper.pdf >.
[REF-10]Santos, J. C. S., Peruma, A., Mirakhorli, M., Galster, M. and Sejfia, A.. "Understanding Software Vulnerabilities Related to Architectural Security Tactics: An Empirical Investigation of Chromium, PHP and Thunderbird.". 2017 IEEE International Conference on Software Architecture (ICSA). 2017. < https://design.se.rit.edu/papers/TacticalVulnerabilities.pdf >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	223	out of	940
Categories	12	out of	374
Views	0	out of	51
Total	235	out of	1365

View ID : 1026
Type : Graph

Objective

CWE nodes in this view (graph) are associated with the OWASP Top Ten, as released in 2017.

Audience

Software Developers

This view outlines the most important issues as identified by the OWASP Top Ten (2017 version), providing a good starting point for web application developers who want to code more securely.

Product Customers

This view outlines the most important issues as identified by the OWASP Top Ten (2017 version), providing product customers with a way of asking their software development teams to follow minimum expectations for secure code.

Educators

Since the OWASP Top Ten covers the most frequently encountered issues, this view can be used by educators as training material for students.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1027	OWASP Top Ten 2017 Category A1 - Injection	2456
HasMember	C	1028	OWASP Top Ten 2017 Category A2 - Broken Authentication	2457
HasMember	C	1029	OWASP Top Ten 2017 Category A3 - Sensitive Data Exposure	2457
HasMember	C	1030	OWASP Top Ten 2017 Category A4 - XML External Entities (XXE)	2458
HasMember	C	1031	OWASP Top Ten 2017 Category A5 - Broken Access Control	2458
HasMember	C	1032	OWASP Top Ten 2017 Category A6 - Security Misconfiguration	2459
HasMember	C	1033	OWASP Top Ten 2017 Category A7 - Cross-Site Scripting (XSS)	2459
HasMember	C	1034	OWASP Top Ten 2017 Category A8 - Insecure Deserialization	2459
HasMember	C	1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities	2460
HasMember	C	1036	OWASP Top Ten 2017 Category A10 - Insufficient Logging & Monitoring	2460

Notes

Relationship

The relationships in this view have been pulled directly from the 2017 OWASP Top 10 document, either from the explicit mapping section, or from weakness types alluded to in the written sections.

References

[REF-957]"Top 10 2017". 2017 April 2. OWASP. < https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	41	out of	940
Categories	12	out of	374

	CWEs in this view		Total CWEs
Views	0	out of	51
Total	53	out of	1365

View-1040: Quality Weaknesses with Indirect Security Impacts

View ID : 1040
Type : Implicit

Objective

CWE identifiers in this view (slice) are quality issues that only indirectly make it easier to introduce a vulnerability and/or make the vulnerability more difficult to detect or mitigate.

Audience

Assessment Tool Vendors

This view makes it easier for assessment vendors to identify and improve coverage for quality-related weaknesses.

Software Developers

This view makes it easier for developers to identify and learn about issues that might make their code more difficult to maintain, perform efficiently or reliably, or secure.

Product Vendors

This view makes it easier for software vendors to identify important issues that may make their software more difficult to maintain, perform efficiently or reliably, or secure.

Filter

/Weakness_Catalog/Weaknesses/Weakness[Weakness_Ordinalities/Weakness_Ordinality/Ordinality='Indirect']

Membership

Nature	Type	ID	Name	Page
HasMember	V	1040	Quality Weaknesses with Indirect Security Impacts	2601

Metrics

	CWEs in this view		Total CWEs
Weaknesses	112	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	112	out of	1365

View-1081: Entries with Maintenance Notes

View ID : 1081
Type : Implicit

Objective

CWE entries in this view have maintenance notes. Maintenance notes are an indicator that an entry might change significantly in future versions. This view was created due to feedback from the CWE Board and participants in the CWE Compatibility Summit in March 2021.

Audience

Assessment Tool Vendors

Assessment vendors may use this view to anticipate future changes to CWE that will help them to better prepare customers for important changes in CWE.

Filter

/Weakness_Catalog/*/*[Notes/Note[@Type='Maintenance']]

Membership

Nature	Type	ID	Name	Page
HasMember	V	1081	Entries with Maintenance Notes	2601

Metrics

	CWEs in this view		Total CWEs
Weaknesses	146	out of	940
Categories	39	out of	374
Views	5	out of	51
Total	190	out of	1365

View-1128: CISQ Quality Measures (2016)

View ID : 1128
Type : Graph

Objective

This view outlines the most important software quality issues as identified by the Consortium for Information & Software Quality (CISQ) Automated Quality Characteristic Measures, released in 2016. These measures are derived from Object Management Group (OMG) standards.

Audience

Software Developers

This view provides a good starting point for anyone involved in software development (including architects, designers, coders, and testers) to ensure that code quality issues are considered during the development process.

Product Vendors

This view can help product vendors understand code quality issues and convey an overall status of their software.

Assessment Tool Vendors

This view provides a good starting point for assessment tool vendors (e.g., vendors selling static analysis tools) who wish to understand what constitutes software with good code quality, and which quality issues may be of concern.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1129	CISQ Quality Measures (2016) - Reliability	2461
HasMember	C	1130	CISQ Quality Measures (2016) - Maintainability	2462
HasMember	C	1131	CISQ Quality Measures (2016) - Security	2463
HasMember	C	1132	CISQ Quality Measures (2016) - Performance Efficiency	2464

References

[REF-968]Consortium for Information & Software Quality (CISQ). "Automated Quality Characteristic Measures". 2016. < http://it-cisq.org/standards/automated-quality-characteristic-measures/ >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	77	out of	940
Categories	4	out of	374
Views	0	out of	51
Total	81	out of	1365

View-1133: Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java

View ID : 1133
Type : Graph

Objective

CWE entries in this view (graph) are fully or partially eliminated by following the guidance presented in the online wiki that reflects that current rules and recommendations of the SEI CERT Oracle Coding Standard for Java.

Audience

Software Developers

By following the SEI CERT Oracle Coding Standard for Java, developers will be able to fully or partially prevent the weaknesses that are identified in this view. In addition, developers can use a CWE coverage graph to determine which weaknesses are not directly addressed by the standard, which will help identify and resolve remaining gaps in training, tool acquisition, or other approaches for reducing weaknesses.

Product Customers

If a software developer claims to be following the SEI CERT Oracle Secure Coding Standard for Java, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could link them to the relevant Secure Coding Standard.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1134	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 00. Input Validation and Data Sanitization (IDS)	2465
HasMember	C	1135	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 01. Declarations and Initialization (DCL)	2465
HasMember	C	1136	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 02. Expressions (EXP)	2466
HasMember	C	1137	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 03. Numeric Types and Operations (NUM)	2466
HasMember	C	1138	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 04. Characters and Strings (STR)	2467
HasMember	C	1139	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 05. Object Orientation (OBJ)	2467
HasMember	C	1140	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 06. Methods (MET)	2468
HasMember	C	1141	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 07. Exceptional Behavior (ERR)	2469
HasMember	C	1142	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 08. Visibility and Atomicity (VNA)	2469

Nature	Type	ID	Name	Page
HasMember	C	1143	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 09. Locking (LCK)	2470
HasMember	C	1144	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 10. Thread APIs (THI)	2470
HasMember	C	1145	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 11. Thread Pools (TPS)	2471
HasMember	C	1146	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 12. Thread-Safety Miscellaneous (TSM)	2471
HasMember	C	1147	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 13. Input Output (FIO)	2471
HasMember	C	1148	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 14. Serialization (SER)	2472
HasMember	C	1149	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 15. Platform Security (SEC)	2473
HasMember	C	1150	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 16. Runtime Environment (ENV)	2473
HasMember	C	1151	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 17. Java Native Interface (JNI)	2474
HasMember	C	1152	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 49. Miscellaneous (MSC)	2474
HasMember	C	1153	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 50. Android (DRD)	2475
HasMember	C	1175	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 18. Concurrency (CON)	2485

Notes

Relationship

The relationships in this view were determined based on specific statements within the rules from the standard. Not all rules have direct relationships to individual weaknesses, although they likely have chaining relationships in specific circumstances.

References

[REF-970]The Software Engineering Institute. "SEI CERT Oracle Coding Standard for Java". < https://wiki.sei.cmu.edu/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	88	out of	940
Categories	21	out of	374
Views	0	out of	51
Total	109	out of	1365

View-1154: Weaknesses Addressed by the SEI CERT C Coding Standard

View ID : 1154
Type : Graph

Objective

CWE entries in this view (graph) are fully or partially eliminated by following the guidance presented in the online wiki that reflects that current rules and recommendations of the SEI CERT C Coding Standard.

Audience

Software Developers

By following the SEI CERT C Coding Standard, developers will be able to fully or partially prevent the weaknesses that are identified in this view. In addition, developers can use a CWE coverage graph to determine which weaknesses are not directly addressed by the standard, which will help identify and resolve remaining gaps in training, tool acquisition, or other approaches for reducing weaknesses.

Product Customers

If a software developer claims to be following the SEI CERT C Coding standard, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could link them to the relevant Secure Coding Standard.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1155	SEI CERT C Coding Standard - Guidelines 01. Preprocessor (PRE)	2475
HasMember	C	1156	SEI CERT C Coding Standard - Guidelines 02. Declarations and Initialization (DCL)	2476
HasMember	C	1157	SEI CERT C Coding Standard - Guidelines 03. Expressions (EXP)	2476
HasMember	C	1158	SEI CERT C Coding Standard - Guidelines 04. Integers (INT)	2477
HasMember	C	1159	SEI CERT C Coding Standard - Guidelines 05. Floating Point (FLP)	2478
HasMember	C	1160	SEI CERT C Coding Standard - Guidelines 06. Arrays (ARR)	2478
HasMember	C	1161	SEI CERT C Coding Standard - Guidelines 07. Characters and Strings (STR)	2479
HasMember	C	1162	SEI CERT C Coding Standard - Guidelines 08. Memory Management (MEM)	2479
HasMember	C	1163	SEI CERT C Coding Standard - Guidelines 09. Input Output (FIO)	2480
HasMember	C	1165	SEI CERT C Coding Standard - Guidelines 10. Environment (ENV)	2481
HasMember	C	1166	SEI CERT C Coding Standard - Guidelines 11. Signals (SIG)	2481
HasMember	C	1167	SEI CERT C Coding Standard - Guidelines 12. Error Handling (ERR)	2482
HasMember	C	1168	SEI CERT C Coding Standard - Guidelines 13. Application Programming Interfaces (API)	2483
HasMember	C	1169	SEI CERT C Coding Standard - Guidelines 14. Concurrency (CON)	2483
HasMember	C	1170	SEI CERT C Coding Standard - Guidelines 48. Miscellaneous (MSC)	2484
HasMember	C	1171	SEI CERT C Coding Standard - Guidelines 50. POSIX (POS)	2484
HasMember	C	1172	SEI CERT C Coding Standard - Guidelines 51. Microsoft Windows (WIN)	2485

Notes

Relationship

The relationships in this view were determined based on specific statements within the rules from the standard. Not all rules have direct relationships to individual weaknesses, although they likely have chaining relationships in specific circumstances.

References

[REF-598]The Software Engineering Institute. "SEI CERT C Coding Standard". < https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	78	out of	940
Categories	17	out of	374
Views	0	out of	51
Total	95	out of	1365

View-1178: Weaknesses Addressed by the SEI CERT Perl Coding Standard

View ID : 1178
Type : Graph

Objective

CWE entries in this view (graph) are fully or partially eliminated by following the guidance presented in the online wiki that reflects that current rules and recommendations of the SEI CERT Perl Coding Standard.

Audience

Software Developers

By following the SEI CERT Perl Coding Standard, developers will be able to fully or partially prevent the weaknesses that are identified in this view. In addition, developers can use a CWE coverage graph to determine which weaknesses are not directly addressed by the standard, which will help identify and resolve remaining gaps in training, tool acquisition, or other approaches for reducing weaknesses.

Product Customers

If a software developer claims to be following the SEI CERT Perl Coding Standard, then customers can search for the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could link them to the relevant Secure Coding Standard.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1179	SEI CERT Perl Coding Standard - Guidelines 01. Input Validation and Data Sanitization (IDS)	2486
HasMember	C	1180	SEI CERT Perl Coding Standard - Guidelines 02. Declarations and Initialization (DCL)	2486
HasMember	C	1181	SEI CERT Perl Coding Standard - Guidelines 03. Expressions (EXP)	2487
HasMember	C	1182	SEI CERT Perl Coding Standard - Guidelines 04. Integers (INT)	2487
HasMember	C	1183	SEI CERT Perl Coding Standard - Guidelines 05. Strings (STR)	2488

Nature	Type	ID	Name	Page
HasMember	C	1184	SEI CERT Perl Coding Standard - Guidelines 06. Object-Oriented Programming (OOP)	2488
HasMember	C	1185	SEI CERT Perl Coding Standard - Guidelines 07. File Input and Output (FIO)	2489
HasMember	C	1186	SEI CERT Perl Coding Standard - Guidelines 50. Miscellaneous (MSC)	2489

Notes

Relationship

The relationships in this view were determined based on specific statements within the rules from the standard. Not all rules have direct relationships to individual weaknesses, although they likely have chaining relationships in specific circumstances.

References

[REF-1011]The Software Engineering Institute. "SEI CERT Perl Coding Standard". < https://wiki.sei.cmu.edu/confluence/display/perl/SEI+CERT+Perl+Coding+Standard >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	26	out of	940
Categories	9	out of	374
Views	0	out of	51
Total	35	out of	1365

View-1194: Hardware Design

View ID : 1194
Type : Graph

Objective

This view organizes weaknesses around concepts that are frequently used or encountered in hardware design. Accordingly, this view can align closely with the perspectives of designers, manufacturers, educators, and assessment vendors. It provides a variety of categories that are intended to simplify navigation, browsing, and mapping.

Audience

Hardware Designers

Hardware Designers use this view to better understand potential mistakes that can be made in specific areas of their IP design. The use of concepts with which hardware designers are familiar makes it easier to navigate.

Educators

Educators use this view to teach future professionals about the types of mistakes that are commonly made in hardware design.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1195	Manufacturing and Life Cycle Management Concerns	2490
HasMember	C	1196	Security Flow Issues	2490
HasMember	C	1197	Integration Issues	2491
HasMember	C	1198	Privilege Separation and Access Control Issues	2491
HasMember	C	1199	General Circuit and Logic Design Concerns	2492

Nature	Type	ID	Name	Page
HasMember	C	1201	Core and Compute Issues	2492
HasMember	C	1202	Memory and Storage Issues	2493
HasMember	C	1203	Peripherals, On-chip Fabric, and Interface/IO Problems	2493
HasMember	C	1205	Security Primitives and Cryptography Issues	2494
HasMember	C	1206	Power, Clock, Thermal, and Reset Concerns	2494
HasMember	C	1207	Debug and Test Problems	2495
HasMember	C	1208	Cross-Cutting Problems	2495
HasMember	C	1388	Physical Access Issues and Concerns	2539

Notes

Other

The top level categories in this view represent commonly understood areas/terms within hardware design, and are meant to aid the user in identifying potential related weaknesses. It is possible for the same weakness to exist within multiple different categories.

Other

This view attempts to present weaknesses in a simple and intuitive way. As such it targets a single level of abstraction. It is important to realize that not every CWE will be represented in this view. High-level class weaknesses and low-level variant weaknesses are mostly ignored. However, by exploring the weaknesses that are included, and following the defined relationships, one can find these higher and lower level weaknesses.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	108	out of	940
Categories	13	out of	374
Views	0	out of	51
Total	121	out of	1365

View-1200: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors

View ID : 1200
Type : Graph

Objective

CWE entries in this view are listed in the 2019 CWE Top 25 Most Dangerous Software Errors.

Audience

Software Developers

By following the Top 25, developers will be able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

If a software developer claims to be following the Top 25, then customers can use the weaknesses in this view in order to formulate independent evidence of that claim.

Educators

Educators can use this view in multiple ways. For example, if there is a focus on teaching weaknesses, the educator could focus on the Top 25.

Membership

Nature	Type	ID	Name	Page
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	B	125	Out-of-bounds Read	336
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	511
HasMember	C	269	Improper Privilege Management	653
HasMember	C	287	Improper Authentication	699
HasMember	B	295	Improper Certificate Validation	721
HasMember	B	352	Cross-Site Request Forgery (CSRF)	875
HasMember	C	400	Uncontrolled Resource Consumption	971
HasMember	V	416	Use After Free	1019
HasMember	B	426	Untrusted Search Path	1035
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	B	611	Improper Restriction of XML External Entity Reference	1376
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1559
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1632
HasMember	B	787	Out-of-bounds Write	1669
HasMember	B	798	Use of Hard-coded Credentials	1699

References

[REF-1028]"2019 CWE Top 25 Most Dangerous Software Errors". 2019 September 6. < https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	25	out of	1365

View-1305: CISQ Quality Measures (2020)

View ID : 1305
Type : Graph

Objective

This view outlines the most important software quality issues as identified by the Consortium for Information & Software Quality (CISQ) Automated Quality Characteristic Measures, released in 2020. These measures are derived from Object Management Group (OMG) standards.

Audience

Software Developers

This view provides a good starting point for anyone involved in software development (including architects, designers, coders, and testers) to ensure that code quality issues are considered during the development process.

Product Vendors

This view can help product vendors understand code quality issues and convey an overall status of their software.

Assessment Tool Vendors

This view provides a good starting point for assessment tool vendors (e.g., vendors selling static analysis tools) who wish to understand what constitutes software with good code quality, and which quality issues may be of concern.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1306	CISQ Quality Measures - Reliability	2504
HasMember	C	1307	CISQ Quality Measures - Maintainability	2505
HasMember	C	1308	CISQ Quality Measures - Security	2506
HasMember	C	1309	CISQ Quality Measures - Efficiency	2507

References

[REF-1133]Consortium for Information & Software Quality (CISQ). "Automated Source Code Quality Measures". 2020. < https://www.omg.org/spec/ASCQM/ >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	138	out of	940
Categories	4	out of	374
Views	0	out of	51
Total	142	out of	1365

View-1337: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses

View ID : 1337
Type : Graph

Objective

CWE entries in this view are listed in the 2021 CWE Top 25 Most Dangerous Software Weaknesses.

Audience

Software Developers

By following the CWE Top 25, developers are able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

Customers can use the weaknesses in this view in order to formulate independent evidence of a claim by a product vendor to have eliminated / mitigated the most dangerous weaknesses.

Educators

Educators can use this view to focus curriculum and teachings on the most dangerous weaknesses.

Membership

Nature	Type	ID	Name	Page
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	B	125	Out-of-bounds Read	336
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	511
HasMember	B	276	Incorrect Default Permissions	672
HasMember	C	287	Improper Authentication	699
HasMember	B	306	Missing Authentication for Critical Function	748
HasMember	F	352	Cross-Site Request Forgery (CSRF)	875
HasMember	V	416	Use After Free	1019
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	C	522	Insufficiently Protected Credentials	1234
HasMember	B	611	Improper Restriction of XML External Entity Reference	1376
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1559
HasMember	B	787	Out-of-bounds Write	1669
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	C	862	Missing Authorization	1789
HasMember	B	918	Server-Side Request Forgery (SSRF)	1829

References

[REF-1185]"2021 CWE Top 25 Most Dangerous Software Weaknesses". 2021 July 0. < https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	25	out of	1365

View-1340: CISQ Data Protection Measures

View ID : 1340
Type : Graph

Objective

This view outlines the SMM representation of the Automated Source Code Data Protection Measurement specifications, as identified by the Consortium for Information & Software Quality (CISQ) Working Group.

Audience

Software Developers

This view provides a good starting point for anyone involved in software development (including architects, designers, coders, and testers) to ensure that code quality issues are considered during the development process.

Product Vendors

This view can help product vendors understand code quality issues and convey an overall status of their software.

Assessment Tool Vendors

This view provides a good starting point for assessment tool vendors (e.g., vendors selling static analysis tools) who wish to understand what constitutes software with good code quality, and which quality issues may be of concern.

Membership

Nature	Type	ID	Name	Page
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	148
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	217
HasMember	B	91	XML Injection (aka Blind XPath Injection)	220
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	249
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	V	129	Improper Validation of Array Index	347
HasMember	B	134	Use of Externally-Controlled Format String	371
HasMember	B	170	Improper Null Termination	434
HasMember	B	213	Exposure of Sensitive Information Due to Incompatible Policies	555
HasMember	P	284	Improper Access Control	687
HasMember	C	311	Missing Encryption of Sensitive Data	764
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	889
HasMember	C	404	Improper Resource Shutdown or Release	987
HasMember	C	424	Improper Protection of Alternate Path	1031
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	B	562	Return of Stack Variable Address	1287
HasMember	B	606	Unchecked Input for Loop Condition	1366
HasMember	B	611	Improper Restriction of XML External Entity Reference	1376

Nature	Type	ID	Name	Page
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1428
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1444
HasMember	C	662	Improper Synchronization	1457
HasMember	C	665	Improper Initialization	1465
HasMember	C	672	Operation on a Resource after Expiration or Release	1488
HasMember	B	681	Incorrect Conversion between Numeric Types	1504
HasMember	P	682	Incorrect Calculation	1507
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1544
HasMember	C	704	Incorrect Type Conversion or Cast	1547
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1559
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	B	908	Use of Uninitialized Resource	1802
HasMember	B	915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	1818
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1896

References

[REF-1157]Consortium for Information & Software Quality (CISQ). "AUTOMATED SOURCE CODE MEASURE FOR DATA PROTECTION". 2020. < https://www.it-cisq.org/automated-source-code-measure-data-protection/index.htm >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	89	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	89	out of	1365

View-1343: Weaknesses in the 2021 CWE Most Important Hardware Weaknesses List

View ID : 1343
Type : Explicit

Objective

CWE entries in this view are listed in the 2021 CWE Most Important Hardware Weaknesses List, as determined by the Hardware CWE Special Interest Group (HW CWE SIG).

Audience

Hardware Designers

By following this list, hardware designers and implementers are able to significantly reduce the number of weaknesses that occur in their products.

Product Customers

Customers can use the weaknesses in this view in order to formulate independent evidence of a claim by a product vendor to have eliminated / mitigated the most dangerous weaknesses.

Educators

Educators can use this view to focus curriculum on the most important hardware weaknesses.

Membership

Nature	Type	ID	Name	Page
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1985
HasMember	B	1191	On-Chip Debug and Test Interface With Improper Access Control	1989
HasMember	B	1231	Improper Prevention of Lock Bit Modification	2018
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	2023
HasMember	B	1240	Use of a Cryptographic Primitive with a Risky Implementation	2036
HasMember	B	1244	Internal Asset Exposed to Unsafe Debug Access Level or State	2048
HasMember	B	1256	Improper Restriction of Software Interfaces to Hardware Features	2076
HasMember	B	1260	Improper Handling of Overlap Between Protected Memory Ranges	2087
HasMember	B	1272	Sensitive Information Uncleared Before Debug/Power State Transition	2116
HasMember	B	1274	Improper Access Control for Volatile Memory Containing Boot Code	2121
HasMember	B	1277	Firmware Not Updateable	2128
HasMember	B	1300	Improper Protection of Physical Side Channels	2177

References

[REF-1238]MITRE. "2021 CWE Most Important Hardware Weaknesses". 2021 October 8. < https://cwe.mitre.org/scoring/lists/2021_CWE_MiHW.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	12	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	12	out of	1365

View-1344: Weaknesses in OWASP Top Ten (2021)

View ID : 1344
Type : Graph

Objective

CWE entries in this view (graph) are associated with the OWASP Top Ten, as released in 2021.

Audience

Software Developers

This view outlines the most important issues as identified by the OWASP Top Ten (2021 version), providing a good starting point for web application developers who want to code more securely.

Product Customers

This view outlines the most important issues as identified by the OWASP Top Ten (2021 version), providing product customers with a way of asking their software development teams to follow minimum expectations for secure code.

Educators

Since the OWASP Top Ten covers the most frequently encountered issues, this view can be used by educators as training material for students.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1345	OWASP Top Ten 2021 Category A01:2021 - Broken Access Control	2508
HasMember	C	1346	OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures	2509
HasMember	C	1347	OWASP Top Ten 2021 Category A03:2021 - Injection	2511
HasMember	C	1348	OWASP Top Ten 2021 Category A04:2021 - Insecure Design	2512
HasMember	C	1349	OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration	2514
HasMember	C	1352	OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components	2515
HasMember	C	1353	OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures	2515
HasMember	C	1354	OWASP Top Ten 2021 Category A08:2021 - Software and Data Integrity Failures	2516
HasMember	C	1355	OWASP Top Ten 2021 Category A09:2021 - Security Logging and Monitoring Failures	2517
HasMember	C	1356	OWASP Top Ten 2021 Category A10:2021 - Server-Side Request Forgery (SSRF)	2518

Notes

Maintenance

As of CWE 4.6, the relationships in this view were pulled directly from the CWE mappings cited in the 2021 OWASP Top Ten. These mappings include categories and high-level weaknesses. One mapping to a deprecated entry was removed. The CWE Program will work with OWASP to improve these mappings, possibly requiring modifications to CWE itself.

References

[REF-1206]"OWASP Top 10:2021". 2021 September 4. OWASP. < https://owasp.org/Top10/ >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	182	out of	940
Categories	23	out of	374
Views	0	out of	51
Total	205	out of	1365

View-1350: Weaknesses in the 2020 CWE Top 25 Most Dangerous Software Weaknesses

View ID : 1350
Type : Graph

Objective

CWE entries in this view are listed in the 2020 CWE Top 25 Most Dangerous Software Weaknesses.

Audience

Software Developers

By following the CWE Top 25, developers are able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

Customers can use the weaknesses in this view in order to formulate independent evidence of a claim by a product vendor to have eliminated / mitigated the most dangerous weaknesses.

Educators

Educators can use this view to focus curriculum and teachings on the most dangerous weaknesses.

Membership

Nature	Type	ID	Name	Page
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	B	125	Out-of-bounds Read	336
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	511
HasMember	C	269	Improper Privilege Management	653
HasMember	C	287	Improper Authentication	699
HasMember	B	306	Missing Authentication for Critical Function	748
HasMember	F	352	Cross-Site Request Forgery (CSRF)	875
HasMember	C	400	Uncontrolled Resource Consumption	971
HasMember	V	416	Use After Free	1019
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	C	522	Insufficiently Protected Credentials	1234
HasMember	B	611	Improper Restriction of XML External Entity Reference	1376
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1559
HasMember	B	787	Out-of-bounds Write	1669
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	C	862	Missing Authorization	1789

References

[REF-1132]"2020 CWE Top 25 Most Dangerous Software Weaknesses". 2020 August 0. < https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374

	CWEs in this view		Total CWEs
Views	0	out of	51
Total	25	out of	1365

View-1358: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS

View ID : 1358
Type : Graph

Objective

CWE entries in this view (graph) are associated with the Categories of Security Vulnerabilities in ICS, as published by the Securing Energy Infrastructure Executive Task Force (SEI ETF) in March 2022. Weaknesses and categories in this view are focused on issues that affect ICS (Industrial Control Systems) but have not been traditionally covered by CWE in the past due to its earlier emphasis on enterprise IT software. Note: weaknesses in this view are based on "Nearest IT Neighbor" recommendations and other suggestions by the CWE team. These relationships are likely to change in future CWE versions.

Audience

Hardware Designers

ICS/OT hardware designers can use this view to ensure a minimal set of weaknesses that should be avoided or mitigated during the design process.

Product Vendors

Product vendors can use this view to ensure that all aspects of the product lifecycle address these weaknesses.

Assessment Tool Vendors

Assessment tool vendors that help to assess potential weaknesses, or avoid them, can use this view to improve their tool's coverage to address more weaknesses.

Academic Researchers

Academic researchers can use this view to identify potential research opportunities that could produce better methods for detection or avoidance of weaknesses in ICS/OT products.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1359	ICS Communications	2518
HasMember	C	1360	ICS Dependencies (& Architecture)	2519
HasMember	C	1361	ICS Supply Chain	2520
HasMember	C	1362	ICS Engineering (Constructions/Deployment)	2520
HasMember	C	1363	ICS Operations (& Maintenance)	2521

Notes

Relationship

Relationships in this view are not authoritative and subject to change. See Maintenance notes.

Maintenance

This view was created in CWE 4.7 to facilitate and illuminate discussion about weaknesses in ICS with [REF-1248] as a starting point. After the release of CWE 4.9 in October 2022, this has been under active review by members of the "Boosting CWE" subgroup of the CWE-CAPEC ICS/OT Special Interest Group (SIG). Relationships are still subject to change. In addition, there may

be some issues in [REF-1248] that are outside of the current scope of CWE, which will require consultation with many CWE stakeholders to resolve.

References

[REF-1248]Securing Energy Infrastructure Executive Task Force (SEI ETF). "Categories of Security Vulnerabilities in ICS". 2022 March 9. < https://inl.gov/wp-content/uploads/2022/03/SEI-ETF-NCSV-TPT-Categories-of-Security-Vulnerabilities-ICS-v1_03-09-22.pdf >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	81	out of	940
Categories	26	out of	374
Views	0	out of	51
Total	107	out of	1365

View-1387: Weaknesses in the 2022 CWE Top 25 Most Dangerous Software Weaknesses

View ID : 1387
Type : Graph

Objective

CWE entries in this view are listed in the 2022 CWE Top 25 Most Dangerous Software Weaknesses.

Audience

Software Developers

By following the CWE Top 25, developers are able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

Customers can use the weaknesses in this view in order to formulate independent evidence of a claim by a product vendor to have eliminated / mitigated the most dangerous weaknesses.

Educators

Educators can use this view to focus curriculum and teachings on the most dangerous weaknesses.

Membership

Nature	Type	ID	Name	Page
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299

Nature	Type	ID	Name	Page
HasMember	B	125	Out-of-bounds Read	336
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	B	276	Incorrect Default Permissions	672
HasMember	C	287	Improper Authentication	699
HasMember	B	306	Missing Authentication for Critical Function	748
HasMember	B	352	Cross-Site Request Forgery (CSRF)	875
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	895
HasMember	C	400	Uncontrolled Resource Consumption	971
HasMember	V	416	Use After Free	1019
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	B	611	Improper Restriction of XML External Entity Reference	1376
HasMember	B	787	Out-of-bounds Write	1669
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	C	862	Missing Authorization	1789
HasMember	B	918	Server-Side Request Forgery (SSRF)	1829

References

[REF-1268]"2022 CWE Top 25 Most Dangerous Software Weaknesses". 2022 June 8. < https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	25	out of	1365

View-1400: Comprehensive Categorization for Software Assurance Trends

View ID : 1400
Type : Graph

Objective

This view organizes weaknesses around categories that are of interest to large-scale software assurance research to support the elimination of weaknesses using tactics such as secure language development. It is also intended to help tracking weakness trends in publicly disclosed vulnerability data. This view is comprehensive in that every weakness must be contained in it, unlike most other views that only use a subset of weaknesses. This view is structured with categories at the top level, with a second level of only weaknesses. Relationships among the weaknesses presented under the research view (CWE-1000) are not shown.

Each weakness is added to only one category. All categories are mutually exclusive; that is, no weakness can be a member of more than one category. While weaknesses defy strict categorization along only one characteristic, the forced bucketing into a single category can simplify certain kinds of analysis.

Note that the size of each category can vary widely because (1) CWE is not as well fleshed-out in some areas compared to others; (2) abstraction of the CWEs in the grouping might go down to Variant level for some buckets, versus others.

Audience

Academic Researchers

Researchers can use this view to evaluate the breadth and depth of software assurance with respect to mitigating and managing weaknesses before they become vulnerabilities.

Membership

Nature	Type	ID	Name	Page
HasMember	C	1396	Comprehensive Categorization: Access Control	2540
HasMember	C	1397	Comprehensive Categorization: Comparison	2544
HasMember	C	1398	Comprehensive Categorization: Component Interaction	2545
HasMember	C	1399	Comprehensive Categorization: Memory Safety	2546
HasMember	C	1401	Comprehensive Categorization: Concurrency	2547
HasMember	C	1402	Comprehensive Categorization: Encryption	2548
HasMember	C	1403	Comprehensive Categorization: Exposed Resource	2549
HasMember	C	1404	Comprehensive Categorization: File Handling	2550
HasMember	C	1405	Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions	2552
HasMember	C	1406	Comprehensive Categorization: Improper Input Validation	2552
HasMember	C	1407	Comprehensive Categorization: Improper Neutralization	2553
HasMember	C	1408	Comprehensive Categorization: Incorrect Calculation	2555
HasMember	C	1409	Comprehensive Categorization: Injection	2556
HasMember	C	1410	Comprehensive Categorization: Insufficient Control Flow Management	2557
HasMember	C	1411	Comprehensive Categorization: Insufficient Verification of Data Authenticity	2559
HasMember	C	1412	Comprehensive Categorization: Poor Coding Practices	2559
HasMember	C	1413	Comprehensive Categorization: Protection Mechanism Failure	2563
HasMember	C	1414	Comprehensive Categorization: Randomness	2564
HasMember	C	1415	Comprehensive Categorization: Resource Control	2565
HasMember	C	1416	Comprehensive Categorization: Resource Lifecycle Management	2566
HasMember	C	1417	Comprehensive Categorization: Sensitive Information Exposure	2569
HasMember	C	1418	Comprehensive Categorization: Violation of Secure Design Principles	2570

Notes

Relationship

This view is different than the software development view (CWE-699) because this view is expected to include all weaknesses regardless of abstraction, while view 699 uses a largely-fixed Base level of abstraction related only to software weaknesses. It is different from the Research view (CWE-1000) because while comprehensive for all weaknesses, the view uses a deep hierarchical structure and excludes categories.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	940	out of	940
Categories	22	out of	374
Views	0	out of	51
Total	962	out of	1365

View-1424: Weaknesses Addressed by ISA/IEC 62443 Requirements

View ID : 1424
Type : Implicit

Objective

This view (slice) covers weaknesses that are addressed by following requirements in the ISA/IEC 62443 series of standards for industrial automation and control systems (IACS). Members of the CWE ICS/OT SIG analyzed a set of CWEs and mapped them to specific requirements covered by ISA/IEC 62443. These mappings are recorded in Taxonomy_Mapping elements.

Filter

/Weakness_Catalog/Weaknesses/Weakness[./Taxonomy_Mappings/Taxonomy_Mapping/@Taxonomy_Name='ISA/IEC 62443']

Membership

Nature	Type	ID	Name	Page
HasMember	V	1424	Weaknesses Addressed by ISA/IEC 62443 Requirements	2621

Notes

Maintenance

The Taxonomy_Mappings to ISA/IEC 62443 were added between CWE 4.9 and CWE 4.14, but some mappings are still under review and might change in future CWE versions. These draft mappings were performed by members of the "Mapping CWE to 62443" subgroup of the CWE ICS/OT Special Interest Group (SIG).

Metrics

	CWEs in this view		Total CWEs
Weaknesses	39	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	39	out of	1365

View-1425: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses

View ID : 1425
Type : Graph

Objective

CWE entries in this view are listed in the 2023 CWE Top 25 Most Dangerous Software Weaknesses.

Audience

Software Developers

By following the CWE Top 25, developers are able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

Customers can use the weaknesses in this view in order to formulate independent evidence of a claim by a product vendor to have eliminated / mitigated the most dangerous weaknesses.

Educators

Educators can use this view to focus curriculum and teachings on the most dangerous weaknesses.

Membership

Nature	Type	ID	Name	Page
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	B	125	Out-of-bounds Read	336
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	C	269	Improper Privilege Management	653
HasMember	B	276	Incorrect Default Permissions	672
HasMember	C	287	Improper Authentication	699
HasMember	B	306	Missing Authentication for Critical Function	748
HasMember	F	352	Cross-Site Request Forgery (CSRF)	875
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	895
HasMember	V	416	Use After Free	1019
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	B	787	Out-of-bounds Write	1669
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	C	862	Missing Authorization	1789
HasMember	C	863	Incorrect Authorization	1796
HasMember	B	918	Server-Side Request Forgery (SSRF)	1829

References

[REF-1344]"2023 CWE Top 25 Most Dangerous Software Weaknesses". 2023 June 9. < https://cwe.mitre.org/top25/archive/2023/2023_cwe_top25.html >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	25	out of	1365

View-1430: Weaknesses in the 2024 CWE Top 25 Most Dangerous Software Weaknesses

View ID : 1430
Type : Graph

Objective

CWE entries in this view are listed in the 2024 CWE Top 25 Most Dangerous Software Weaknesses.

Audience

Software Developers

By following the CWE Top 25, developers are able to significantly reduce the number of weaknesses that occur in their software.

Product Customers

Customers can use the weaknesses in this view in order to formulate independent evidence of a claim by a product vendor to have eliminated / mitigated the most dangerous weaknesses.

Educators

Educators can use this view to focus curriculum and teachings on the most dangerous weaknesses.

Membership

Nature	Type	ID	Name	Page
HasMember	C	20	Improper Input Validation	20
HasMember	B	22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	33
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	148
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	155
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	168
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	206
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	225
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	299
HasMember	B	125	Out-of-bounds Read	336
HasMember	B	190	Integer Overflow or Wraparound	478
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	511
HasMember	C	269	Improper Privilege Management	653
HasMember	C	287	Improper Authentication	699
HasMember	B	306	Missing Authentication for Critical Function	748
HasMember		352	Cross-Site Request Forgery (CSRF)	875
HasMember	C	400	Uncontrolled Resource Consumption	971
HasMember	V	416	Use After Free	1019
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1055
HasMember	B	476	NULL Pointer Dereference	1139
HasMember	B	502	Deserialization of Untrusted Data	1212
HasMember	B	787	Out-of-bounds Write	1669
HasMember	B	798	Use of Hard-coded Credentials	1699
HasMember	C	862	Missing Authorization	1789
HasMember	C	863	Incorrect Authorization	1796
HasMember	B	918	Server-Side Request Forgery (SSRF)	1829

References

[REF-1453]"2024 CWE Top 25 Most Dangerous Software Weaknesses". 2024 November 9. < https://cwe.mitre.org/top25 >.2024-11-17.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	940
Categories	0	out of	374
Views	0	out of	51
Total	25	out of	1365

View-2000: Comprehensive CWE Dictionary

View ID : 2000
Type : Implicit

Objective

This view (slice) covers all the elements in CWE.

Filter

/Weakness_Catalog/*[not(self::External_References)]/*

Membership

Nature	Type	ID	Name	Page
HasMember	V	2000	Comprehensive CWE Dictionary	2624

Metrics

	CWEs in this view		Total CWEs
Weaknesses	940	out of	940
Categories	374	out of	374
Views	51	out of	51
Total	1365	out of	1365

Graph View: CWE-629: Weaknesses in OWASP Top Ten (2007)

- CWE-712: OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS) *(p.2351)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
- CWE-713: OWASP Top Ten 2007 Category A2 - Injection Flaws *(p.2351)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.148)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.217)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.220)*
  - CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.222)*
- CWE-714: OWASP Top Ten 2007 Category A3 - Malicious File Execution *(p.2352)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1055)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.232)*
  - CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.242)*
- CWE-715: OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference *(p.2352)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1131)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
- CWE-716: OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF) *(p.2353)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.875)*
- CWE-717: OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling *(p.2353)*
  - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.511)*
  - CWE-203: Observable Discrepancy *(p.525)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.558)*
- CWE-718: OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management *(p.2353)*
  - CWE-287: Improper Authentication *(p.699)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.740)*
  - CWE-522: Insufficiently Protected Credentials *(p.1234)*
- CWE-719: OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage *(p.2354)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.792)*
  - CWE-325: Missing Cryptographic Step *(p.801)*
  - CWE-326: Inadequate Encryption Strength *(p.803)*
- CWE-720: OWASP Top Ten 2007 Category A9 - Insecure Communications *(p.2354)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.792)*
  - CWE-325: Missing Cryptographic Step *(p.801)*
  - CWE-326: Inadequate Encryption Strength *(p.803)*
- CWE-721: OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access *(p.2355)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.707)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*

Graph View: CWE-631: DEPRECATED: Resource-specific Weaknesses

Graph View: CWE-699: Software Development

- CWE-1228: API / Function Errors *(p.2503)*
  - CWE-242: Use of Inherently Dangerous Function *(p.593)*
  - CWE-474: Use of Function with Inconsistent Implementations *(p.1136)*
  - CWE-475: Undefined Behavior for Input to API *(p.1138)*
  - CWE-477: Use of Obsolete Function *(p.1146)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1498)*
  - CWE-695: Use of Low-Level Functionality *(p.1533)*
  - CWE-749: Exposed Dangerous Method or Function *(p.1572)*
- CWE-1210: Audit / Logging Errors *(p.2496)*
  - CWE-117: Improper Output Neutralization for Logs *(p.294)*
  - CWE-222: Truncation of Security-relevant Information *(p.565)*
  - CWE-223: Omission of Security-relevant Information *(p.566)*
  - CWE-224: Obscured Security-relevant Information by Alternate Name *(p.568)*
  - CWE-778: Insufficient Logging *(p.1647)*
  - CWE-779: Logging of Excessive Data *(p.1651)*
- CWE-1211: Authentication Errors *(p.2496)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.710)*
  - CWE-290: Authentication Bypass by Spoofing *(p.712)*
  - CWE-294: Authentication Bypass by Capture-replay *(p.719)*
  - CWE-295: Improper Certificate Validation *(p.721)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.740)*
  - CWE-303: Incorrect Implementation of Authentication Algorithm *(p.744)*
  - CWE-305: Authentication Bypass by Primary Weakness *(p.747)*
  - CWE-306: Missing Authentication for Critical Function *(p.748)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.754)*
  - CWE-308: Use of Single-factor Authentication *(p.759)*
  - CWE-309: Use of Password System for Primary Authentication *(p.761)*
  - CWE-322: Key Exchange without Entity Authentication *(p.795)*
  - CWE-603: Use of Client-Side Authentication *(p.1363)*
  - CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1432)*
  - CWE-804: Guessable CAPTCHA *(p.1710)*
  - CWE-836: Use of Password Hash Instead of Password for Authentication *(p.1770)*
- CWE-1212: Authorization Errors *(p.2497)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1273)*
  - CWE-552: Files or Directories Accessible to External Parties *(p.1274)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
  - CWE-653: Improper Isolation or Compartmentalization *(p.1445)*
  - CWE-939: Improper Authorization in Handler for Custom URL Scheme *(p.1849)*
  - CWE-842: Placement of User into Incorrect Group *(p.1784)*
  - CWE-1220: Insufficient Granularity of Access Control *(p.2002)*
  - CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2017)*
- CWE-1006: Bad Coding Practices *(p.2443)*
  - CWE-358: Improperly Implemented Security Check for Standard *(p.888)*
  - CWE-360: Trust of System Event Data *(p.894)*
  - CWE-478: Missing Default Case in Multiple Condition Expression *(p.1149)*
  - CWE-487: Reliance on Package-level Scope *(p.1175)*
  - CWE-489: Active Debug Code *(p.1178)*
  - CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1267)*
  - CWE-561: Dead Code *(p.1283)*
  - CWE-562: Return of Stack Variable Address *(p.1287)*
  - CWE-563: Assignment to Variable without Use *(p.1289)*
  - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1321)*

- CWE-586: Explicit Call to Finalize() *(p.1329)*
- CWE-605: Multiple Binds to the Same Port *(p.1364)*
- CWE-628: Function Call with Incorrectly Specified Arguments *(p.1407)*
- CWE-654: Reliance on a Single Factor in a Security Decision *(p.1448)*
- CWE-656: Reliance on Security Through Obscurity *(p.1452)*
- CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1531)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1723)*
- CWE-1041: Use of Redundant Code *(p.1884)*
- CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1887)*
- CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range *(p.1888)*
- CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor *(p.1889)*
- CWE-1046: Creation of Immutable Text Using String Concatenation *(p.1890)*
- CWE-1048: Invokable Control Element with Large Number of Outward Calls *(p.1892)*
- CWE-1049: Excessive Data Query Operations in a Large Data Table *(p.1894)*
- CWE-1050: Excessive Platform Resource Consumption within a Loop *(p.1895)*
- CWE-1063: Creation of Class Instance within a Static Code Block *(p.1910)*
- CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers *(p.1912)*
- CWE-1066: Missing Serialization Control Element *(p.1913)*
- CWE-1067: Excessive Execution of Sequential Searches of Data Resource *(p.1914)*
- CWE-1070: Serializable Data Element Containing non-Serializable Item Elements *(p.1918)*
- CWE-1071: Empty Code Block *(p.1919)*
- CWE-1072: Data Resource Access without Use of Connection Pooling *(p.1921)*
- CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses *(p.1922)*
- CWE-1079: Parent Class without Virtual Destructor Method *(p.1929)*
- CWE-1082: Class Instance Self Destruction Control Element *(p.1931)*
- CWE-1084: Invokable Control Element with Excessive File or Data Access Operations *(p.1933)*
- CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code *(p.1934)*
- CWE-1087: Class with Virtual Method without a Virtual Destructor *(p.1936)*
- CWE-1089: Large Data Table with Excessive Number of Indices *(p.1938)*
- CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers *(p.1941)*
- CWE-1094: Excessive Index Range Scan for a Data Resource *(p.1943)*
- CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element *(p.1946)*
- CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element *(p.1947)*
- CWE-1099: Inconsistent Naming Conventions for Identifiers *(p.1948)*
- CWE-1101: Reliance on Runtime Component in Generated Code *(p.1950)*
- CWE-1102: Reliance on Machine-Dependent Data Representation *(p.1951)*
- CWE-1103: Use of Platform-Dependent Third Party Components *(p.1952)*
- CWE-1104: Use of Unmaintained Third Party Components *(p.1953)*
- CWE-1106: Insufficient Use of Symbolic Constants *(p.1955)*
- CWE-1107: Insufficient Isolation of Symbolic Constant Definitions *(p.1956)*
- CWE-1108: Excessive Reliance on Global Variables *(p.1957)*
- CWE-1109: Use of Same Variable for Multiple Purposes *(p.1958)*
- CWE-1113: Inappropriate Comment Style *(p.1962)*
- CWE-1114: Inappropriate Whitespace Style *(p.1963)*
- CWE-1115: Source Code Element without Standard Prologue *(p.1963)*
- CWE-1116: Inaccurate Comments *(p.1964)*
- CWE-1117: Callable with Insufficient Behavioral Summary *(p.1966)*
- CWE-1126: Declaration of Variable with Unnecessarily Wide Scope *(p.1975)*
- CWE-1127: Compilation with Insufficient Warnings or Errors *(p.1976)*
- CWE-1235: Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations *(p.2029)*

- CWE-438: Behavioral Problems *(p.2348)*
  - CWE-115: Misinterpretation of Input *(p.286)*
  - CWE-179: Incorrect Behavior Order: Early Validation *(p.454)*
  - CWE-408: Incorrect Behavior Order: Early Amplification *(p.1002)*
  - CWE-437: Incomplete Model of Endpoint Features *(p.1067)*
  - CWE-439: Behavioral Change in New Version or Environment *(p.1068)*
  - CWE-440: Expected Behavior Violation *(p.1069)*
  - CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1075)*
  - CWE-480: Use of Incorrect Operator *(p.1157)*
  - CWE-483: Incorrect Block Delimitation *(p.1167)*
  - CWE-484: Omitted Break Statement in Switch *(p.1169)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1273)*
  - CWE-698: Execution After Redirect (EAR) *(p.1542)*
  - CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1570)*
  - CWE-783: Operator Precedence Logic Error *(p.1659)*
  - CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1766)*
  - CWE-837: Improper Enforcement of a Single, Unique Action *(p.1771)*
  - CWE-841: Improper Enforcement of Behavioral Workflow *(p.1781)*
  - CWE-1025: Comparison Using Wrong Factors *(p.1878)*
  - CWE-1037: Processor Optimization Removal or Modification of Security-critical Code *(p.1879)*
- CWE-840: Business Logic Errors *(p.2381)*
  - CWE-283: Unverified Ownership *(p.685)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1418)*
  - CWE-708: Incorrect Ownership Assignment *(p.1556)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*
  - CWE-826: Premature Release of Resource During Expected Lifetime *(p.1743)*
  - CWE-837: Improper Enforcement of a Single, Unique Action *(p.1771)*
  - CWE-841: Improper Enforcement of Behavioral Workflow *(p.1781)*
- CWE-417: Communication Channel Errors *(p.2347)*
  - CWE-322: Key Exchange without Entity Authentication *(p.795)*
  - CWE-346: Origin Validation Error *(p.860)*
  - CWE-385: Covert Timing Channel *(p.947)*
  - CWE-419: Unprotected Primary Channel *(p.1024)*
  - CWE-420: Unprotected Alternate Channel *(p.1025)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
  - CWE-515: Covert Storage Channel *(p.1229)*
  - CWE-918: Server-Side Request Forgery (SSRF) *(p.1829)*
  - CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1839)*
  - CWE-940: Improper Verification of Source of a Communication Channel *(p.1852)*
  - CWE-941: Incorrectly Specified Destination in a Communication Channel *(p.1855)*
  - CWE-1327: Binding to an Unrestricted IP Address *(p.2227)*
- CWE-1226: Complexity Issues *(p.2502)*
  - CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1887)*
  - CWE-1047: Modules with Circular Dependencies *(p.1891)*
  - CWE-1055: Multiple Inheritance from Concrete Classes *(p.1900)*
  - CWE-1056: Invokable Control Element with Variadic Parameters *(p.1901)*
  - CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses *(p.1906)*
  - CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters *(p.1911)*
  - CWE-1074: Class with Excessively Deep Inheritance *(p.1923)*
  - CWE-1075: Unconditional Control Flow Transfer outside of Switch Block *(p.1924)*

- CWE-1080: Source Code File with Excessive Number of Lines of Code *(p.1930)*
- CWE-1086: Class with Excessive Number of Child Classes *(p.1935)*
- CWE-1095: Loop Condition Value Update within the Loop *(p.1944)*
- CWE-1119: Excessive Use of Unconditional Branching *(p.1968)*
- CWE-1121: Excessive McCabe Cyclomatic Complexity *(p.1970)*
- CWE-1122: Excessive Halstead Complexity *(p.1971)*
- CWE-1123: Excessive Use of Self-Modifying Code *(p.1972)*
- CWE-1124: Excessively Deep Nesting *(p.1973)*
- CWE-1125: Excessive Attack Surface *(p.1974)*
- CWE-1333: Inefficient Regular Expression Complexity *(p.2243)*

CWE-557: Concurrency Issues *(p.2350)*
- CWE-364: Signal Handler Race Condition *(p.905)*
- CWE-366: Race Condition within a Thread *(p.910)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.913)*
- CWE-368: Context Switching Race Condition *(p.918)*
- CWE-386: Symbolic Name not Mapping to Correct Object *(p.949)*
- CWE-421: Race Condition During Access to Alternate Channel *(p.1028)*
- CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1461)*
- CWE-820: Missing Synchronization *(p.1729)*
- CWE-821: Incorrect Synchronization *(p.1731)*
- CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1903)*
- CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context *(p.2219)*

CWE-255: Credentials Management Errors *(p.2336)*
- CWE-256: Plaintext Storage of a Password *(p.622)*
- CWE-257: Storing Passwords in a Recoverable Format *(p.625)*
- CWE-260: Password in Configuration File *(p.636)*
- CWE-261: Weak Encoding for Password *(p.638)*
- CWE-262: Not Using Password Aging *(p.640)*
- CWE-263: Password Aging with Long Expiration *(p.643)*
- CWE-324: Use of a Key Past its Expiration Date *(p.799)*
- CWE-521: Weak Password Requirements *(p.1231)*
- CWE-523: Unprotected Transport of Credentials *(p.1239)*
- CWE-549: Missing Password Field Masking *(p.1271)*
- CWE-620: Unverified Password Change *(p.1392)*
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1418)*
- CWE-798: Use of Hard-coded Credentials *(p.1699)*
- CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1822)*
- CWE-1392: Use of Default Credentials *(p.2284)*

CWE-310: Cryptographic Issues *(p.2339)*
- CWE-261: Weak Encoding for Password *(p.638)*
- CWE-324: Use of a Key Past its Expiration Date *(p.799)*
- CWE-325: Missing Cryptographic Step *(p.801)*
- CWE-328: Use of Weak Hash *(p.813)*
- CWE-331: Insufficient Entropy *(p.828)*
- CWE-334: Small Space of Random Values *(p.834)*
- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.836)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.844)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.864)*
- CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1822)*
- CWE-1204: Generation of Weak Initialization Vector (IV) *(p.1996)*
- CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation *(p.2036)*

CWE-320: Key Management Errors *(p.2340)*
- CWE-322: Key Exchange without Entity Authentication *(p.795)*

- CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.797)*
- CWE-324: Use of a Key Past its Expiration Date *(p.799)*
- CWE-798: Use of Hard-coded Credentials *(p.1699)*

CWE-1214: Data Integrity Issues *(p.2498)*
- CWE-322: Key Exchange without Entity Authentication *(p.795)*
- CWE-346: Origin Validation Error *(p.860)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.864)*
- CWE-348: Use of Less Trusted Source *(p.866)*
- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.868)*
- CWE-351: Insufficient Type Distinction *(p.873)*
- CWE-353: Missing Support for Integrity Check *(p.881)*
- CWE-354: Improper Validation of Integrity Check Value *(p.883)*
- CWE-494: Download of Code Without Integrity Check *(p.1192)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1292)*
- CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1439)*
- CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1750)*
- CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1839)*

CWE-19: Data Processing Errors *(p.2330)*
- CWE-130: Improper Handling of Length Parameter Inconsistency *(p.357)*
- CWE-166: Improper Handling of Missing Special Element *(p.429)*
- CWE-167: Improper Handling of Additional Special Element *(p.431)*
- CWE-168: Improper Handling of Inconsistent Special Elements *(p.433)*
- CWE-178: Improper Handling of Case Sensitivity *(p.451)*
- CWE-182: Collapse of Data into Unsafe Value *(p.462)*
- CWE-186: Overly Restrictive Regular Expression *(p.472)*
- CWE-229: Improper Handling of Values *(p.577)*
- CWE-233: Improper Handling of Parameters *(p.581)*
- CWE-237: Improper Handling of Structural Elements *(p.587)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.591)*
- CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.1004)*
- CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1131)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1376)*
- CWE-624: Executable Regular Expression Error *(p.1399)*
- CWE-625: Permissive Regular Expression *(p.1400)*
- CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1642)*
- CWE-1024: Comparison of Incompatible Types *(p.1877)*

CWE-137: Data Neutralization Issues *(p.2332)*
- CWE-76: Improper Neutralization of Equivalent Special Elements *(p.146)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.217)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.220)*
- CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.222)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.225)*
- CWE-117: Improper Output Neutralization for Logs *(p.294)*
- CWE-140: Improper Neutralization of Delimiters *(p.382)*

- CWE-170: Improper Null Termination *(p.434)*
- CWE-463: Deletion of Data Structure Sentinel *(p.1113)*
- CWE-464: Addition of Data Structure Sentinel *(p.1115)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1421)*
- CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1531)*
- CWE-791: Incomplete Filtering of Special Elements *(p.1689)*
- CWE-838: Inappropriate Encoding for Output Context *(p.1773)*
- CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1827)*
- CWE-1236: Improper Neutralization of Formula Elements in a CSV File *(p.2031)*

C CWE-1225: Documentation Issues *(p.2501)*
- CWE-1053: Missing Documentation for Design *(p.1898)*
- CWE-1068: Inconsistency Between Implementation and Documented Design *(p.1915)*
- CWE-1110: Incomplete Design Documentation *(p.1959)*
- CWE-1111: Incomplete I/O Documentation *(p.1960)*
- CWE-1112: Incomplete Documentation of Program Execution *(p.1961)*
- CWE-1118: Insufficient Documentation of Error Handling Techniques *(p.1967)*

C CWE-1219: File Handling Issues *(p.2501)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-41: Improper Resolution of Path Equivalence *(p.87)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.112)*
- CWE-66: Improper Handling of File Names that Identify Virtual Resources *(p.125)*
- CWE-378: Creation of Temporary File With Insecure Permissions *(p.935)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.937)*
- CWE-426: Untrusted Search Path *(p.1035)*
- CWE-427: Uncontrolled Search Path Element *(p.1040)*
- CWE-428: Unquoted Search Path or Element *(p.1047)*

C CWE-1227: Encapsulation Issues *(p.2502)*
- CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer *(p.1899)*
- CWE-1057: Data Access Operations Outside of Expected Data Manager Component *(p.1902)*
- CWE-1062: Parent Class with References to Child Class *(p.1909)*
- CWE-1083: Data Access from Outside Expected Data Manager Component *(p.1932)*
- CWE-1090: Method Containing Access of a Member Element from Another Class *(p.1939)*
- CWE-1100: Insufficient Isolation of System-Dependent Functions *(p.1949)*
- CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality *(p.1954)*

C CWE-389: Error Conditions, Return Values, Status Codes *(p.2344)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
- CWE-248: Uncaught Exception *(p.603)*
- CWE-252: Unchecked Return Value *(p.613)*
- CWE-253: Incorrect Check of Function Return Value *(p.620)*
- CWE-390: Detection of Error Condition Without Action *(p.950)*
- CWE-391: Unchecked Error Condition *(p.955)*
- CWE-392: Missing Report of Error Condition *(p.958)*
- CWE-393: Return of Wrong Status Code *(p.960)*
- CWE-394: Unexpected Status Code or Return Value *(p.962)*
- CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.964)*
- CWE-396: Declaration of Catch for Generic Exception *(p.966)*
- CWE-397: Declaration of Throws for Generic Exception *(p.968)*
- CWE-544: Missing Standardized Error Handling Mechanism *(p.1265)*
- CWE-584: Return Inside Finally Block *(p.1325)*
- CWE-617: Reachable Assertion *(p.1387)*
- CWE-756: Missing Custom Error Page *(p.1588)*

C CWE-569: Expression Issues *(p.2351)*
- CWE-480: Use of Incorrect Operator *(p.1157)*

- CWE-570: Expression is Always False *(p.1300)*
- CWE-571: Expression is Always True *(p.1303)*
- CWE-783: Operator Precedence Logic Error *(p.1659)*

C CWE-429: Handler Errors *(p.2347)*
- CWE-430: Deployment of Wrong Handler *(p.1049)*
- CWE-431: Missing Handler *(p.1051)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1055)*

C CWE-199: Information Management Errors *(p.2333)*
- CWE-201: Insertion of Sensitive Information Into Sent Data *(p.521)*
- CWE-204: Observable Response Discrepancy *(p.530)*
- CWE-205: Observable Behavioral Discrepancy *(p.533)*
- CWE-208: Observable Timing Discrepancy *(p.537)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.551)*
- CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.555)*
- CWE-214: Invocation of Process Using Visible Sensitive Information *(p.556)*
- CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.558)*
- CWE-312: Cleartext Storage of Sensitive Information *(p.771)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.889)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1201)*
- CWE-524: Use of Cache Containing Sensitive Information *(p.1240)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1257)*
- CWE-921: Storage of Sensitive Data in a Mechanism without Access Control *(p.1834)*
- CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2017)*

C CWE-452: Initialization and Cleanup Errors *(p.2348)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.551)*
- CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1092)*
- CWE-455: Non-exit on Failed Initialization *(p.1095)*
- CWE-459: Incomplete Cleanup *(p.1106)*
- CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1896)*
- CWE-1052: Excessive Use of Hard-Coded Literals in Initialization *(p.1897)*
- CWE-1188: Initialization of a Resource with an Insecure Default *(p.1983)*

C CWE-1215: Data Validation Issues *(p.2499)*
- CWE-112: Missing XML Validation *(p.275)*
- CWE-179: Incorrect Behavior Order: Early Validation *(p.454)*
- CWE-183: Permissive List of Allowed Inputs *(p.464)*
- CWE-184: Incomplete List of Disallowed Inputs *(p.466)*
- CWE-606: Unchecked Input for Loop Condition *(p.1366)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1421)*
- CWE-1173: Improper Use of Validation Framework *(p.1978)*
- CWE-1284: Improper Validation of Specified Quantity in Input *(p.2142)*
- CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input *(p.2144)*
- CWE-1286: Improper Validation of Syntactic Correctness of Input *(p.2148)*
- CWE-1287: Improper Validation of Specified Type of Input *(p.2150)*
- CWE-1288: Improper Validation of Consistency within Input *(p.2151)*
- CWE-1289: Improper Validation of Unsafe Equivalence in Input *(p.2153)*

C CWE-1216: Lockout Mechanism Errors *(p.2499)*
- CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1432)*

C CWE-1218: Memory Buffer Errors *(p.2500)*
- CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
- CWE-124: Buffer Underwrite ('Buffer Underflow') *(p.332)*
- CWE-125: Out-of-bounds Read *(p.336)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.361)*

- CWE-786: Access of Memory Location Before Start of Buffer *(p.1666)*
- CWE-787: Out-of-bounds Write *(p.1669)*
- CWE-788: Access of Memory Location After End of Buffer *(p.1678)*
- CWE-805: Buffer Access with Incorrect Length Value *(p.1711)*
- CWE-1284: Improper Validation of Specified Quantity in Input *(p.2142)*

CWE-189: Numeric Errors *(p.2333)*
- CWE-128: Wrap-around Error *(p.345)*
- CWE-190: Integer Overflow or Wraparound *(p.478)*
- CWE-191: Integer Underflow (Wrap or Wraparound) *(p.487)*
- CWE-193: Off-by-one Error *(p.493)*
- CWE-369: Divide By Zero *(p.920)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
- CWE-839: Numeric Range Comparison Without Minimum Check *(p.1776)*
- CWE-1335: Incorrect Bitwise Shift of Integer *(p.2247)*
- CWE-1339: Insufficient Precision or Accuracy of a Real Number *(p.2254)*
- CWE-1389: Incorrect Parsing of Numbers with Different Radices *(p.2275)*

CWE-275: Permission Issues *(p.2339)*
- CWE-276: Incorrect Default Permissions *(p.672)*
- CWE-277: Insecure Inherited Permissions *(p.675)*
- CWE-278: Insecure Preserved Inherited Permissions *(p.676)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.678)*
- CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.679)*
- CWE-281: Improper Preservation of Permissions *(p.681)*
- CWE-618: Exposed Unsafe ActiveX Method *(p.1389)*
- CWE-766: Critical Data Element Declared Public *(p.1615)*
- CWE-767: Access to Critical Private Variable via Public Method *(p.1619)*

CWE-465: Pointer Issues *(p.2349)*
- CWE-466: Return of Pointer Value Outside of Expected Range *(p.1117)*
- CWE-468: Incorrect Pointer Scaling *(p.1121)*
- CWE-469: Use of Pointer Subtraction to Determine Size *(p.1123)*
- CWE-476: NULL Pointer Dereference *(p.1139)*
- CWE-587: Assignment of a Fixed Address to a Pointer *(p.1330)*
- CWE-763: Release of Invalid Pointer or Reference *(p.1608)*
- CWE-822: Untrusted Pointer Dereference *(p.1732)*
- CWE-823: Use of Out-of-range Pointer Offset *(p.1735)*
- CWE-824: Access of Uninitialized Pointer *(p.1738)*
- CWE-825: Expired Pointer Dereference *(p.1741)*

CWE-265: Privilege Issues *(p.2338)*
- CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.596)*
- CWE-250: Execution with Unnecessary Privileges *(p.606)*
- CWE-266: Incorrect Privilege Assignment *(p.645)*
- CWE-267: Privilege Defined With Unsafe Actions *(p.648)*
- CWE-268: Privilege Chaining *(p.651)*
- CWE-270: Privilege Context Switching Error *(p.659)*
- CWE-272: Least Privilege Violation *(p.663)*
- CWE-273: Improper Check for Dropped Privileges *(p.667)*
- CWE-274: Improper Handling of Insufficient Privileges *(p.670)*
- CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.679)*
- CWE-501: Trust Boundary Violation *(p.1210)*
- CWE-580: clone() Method Without super.clone() *(p.1319)*
- CWE-648: Incorrect Use of Privileged APIs *(p.1437)*

CWE-1213: Random Number Issues *(p.2498)*
- CWE-331: Insufficient Entropy *(p.828)*
- CWE-334: Small Space of Random Values *(p.834)*

- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.836)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.844)*
- CWE-341: Predictable from Observable State *(p.850)*
- CWE-342: Predictable Exact Value from Previous Values *(p.852)*
- CWE-343: Predictable Value Range from Previous Values *(p.854)*
- CWE-344: Use of Invariant Value in Dynamically Changing Context *(p.856)*
- CWE-1241: Use of Predictable Algorithm in Random Number Generator *(p.2042)*

CWE-411: Resource Locking Problems *(p.2346)*
- CWE-412: Unrestricted Externally Accessible Lock *(p.1007)*
- CWE-413: Improper Resource Locking *(p.1010)*
- CWE-414: Missing Lock Check *(p.1014)*
- CWE-609: Double-Checked Locking *(p.1371)*
- CWE-764: Multiple Locks of a Critical Resource *(p.1613)*
- CWE-765: Multiple Unlocks of a Critical Resource *(p.1614)*
- CWE-832: Unlock of a Resource that is not Locked *(p.1761)*
- CWE-833: Deadlock *(p.1762)*

CWE-399: Resource Management Errors *(p.2345)*
- CWE-73: External Control of File Name or Path *(p.133)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.985)*
- CWE-410: Insufficient Resource Pool *(p.1005)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1125)*
- CWE-502: Deserialization of Untrusted Data *(p.1212)*
- CWE-619: Dangling Database Cursor ('Cursor Injection') *(p.1391)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1421)*
- CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1531)*
- CWE-763: Release of Invalid Pointer or Reference *(p.1608)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*
- CWE-771: Missing Reference to Active Allocated Resource *(p.1631)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1632)*
- CWE-826: Premature Release of Resource During Expected Lifetime *(p.1743)*
- CWE-908: Use of Uninitialized Resource *(p.1802)*
- CWE-909: Missing Initialization of Resource *(p.1806)*
- CWE-910: Use of Expired File Descriptor *(p.1809)*
- CWE-911: Improper Update of Reference Count *(p.1811)*
- CWE-914: Improper Control of Dynamically-Identified Variables *(p.1816)*
- CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes *(p.1818)*
- CWE-920: Improper Restriction of Power Consumption *(p.1832)*
- CWE-1188: Initialization of a Resource with an Insecure Default *(p.1983)*
- CWE-1341: Multiple Releases of Same Resource or Handle *(p.2258)*

CWE-387: Signal Errors *(p.2343)*
- CWE-364: Signal Handler Race Condition *(p.905)*

CWE-371: State Issues *(p.2342)*
- CWE-15: External Control of System or Configuration Setting *(p.17)*
- CWE-372: Incomplete Internal State Distinction *(p.926)*
- CWE-374: Passing Mutable Objects to an Untrusted Method *(p.927)*
- CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.930)*
- CWE-1265: Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls *(p.2100)*

CWE-133: String Errors *(p.2331)*
- CWE-134: Use of Externally-Controlled Format String *(p.371)*
- CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.377)*
- CWE-480: Use of Incorrect Operator *(p.1157)*

CWE-136: Type Errors *(p.2331)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') *(p.1785)*

- CWE-1287: Improper Validation of Specified Type of Input *(p.2150)*

CWE-355: User Interface Security Issues *(p.2341)*

- CWE-356: Product UI does not Warn User of Unsafe Actions *(p.886)*
- CWE-357: Insufficient UI Warning of Dangerous Operations *(p.887)*
- CWE-447: Unimplemented or Unsupported Feature in UI *(p.1082)*
- CWE-448: Obsolete Feature in UI *(p.1083)*
- CWE-449: The UI Performs the Wrong Action *(p.1084)*
- CWE-549: Missing Password Field Masking *(p.1271)*
- CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User *(p.1866)*
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1869)*

CWE-1217: User Session Errors *(p.2500)*

- CWE-488: Exposure of Data Element to Wrong Session *(p.1176)*
- CWE-613: Insufficient Session Expiration *(p.1380)*
- CWE-841: Improper Enforcement of Behavioral Workflow *(p.1781)*

Graph View: CWE-700: Seven Pernicious Kingdoms

- CWE-254: 7PK - Security Features *(p.2335)*
  - CWE-256: Plaintext Storage of a Password *(p.622)*
  - CWE-258: Empty Password in Configuration File *(p.628)*
  - CWE-259: Use of Hard-coded Password *(p.630)*
  - CWE-260: Password in Configuration File *(p.636)*
  - CWE-261: Weak Encoding for Password *(p.638)*
  - CWE-272: Least Privilege Violation *(p.663)*
  - CWE-284: Improper Access Control *(p.687)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.889)*
  - CWE-798: Use of Hard-coded Credentials *(p.1699)*
- CWE-361: 7PK - Time and State *(p.2341)*
  - CWE-364: Signal Handler Race Condition *(p.905)*
  - CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.913)*
  - CWE-377: Insecure Temporary File *(p.932)*
  - CWE-382: J2EE Bad Practices: Use of System.exit() *(p.940)*
  - CWE-383: J2EE Bad Practices: Direct Use of Threads *(p.942)*
  - CWE-384: Session Fixation *(p.943)*
  - CWE-412: Unrestricted Externally Accessible Lock *(p.1007)*
- CWE-388: 7PK - Errors *(p.2343)*
  - CWE-391: Unchecked Error Condition *(p.955)*
  - CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.964)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.966)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.968)*
- CWE-1005: 7PK - Input Validation and Representation *(p.2442)*
  - CWE-20: Improper Input Validation *(p.20)*
    - CWE-102: Struts: Duplicate Validation Forms *(p.252)*
    - CWE-103: Struts: Incomplete validate() Method Definition *(p.254)*
    - CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.257)*
    - CWE-105: Struts: Form Field Without Validator *(p.259)*
    - CWE-106: Struts: Plug-in Framework not in Use *(p.262)*
    - CWE-107: Struts: Unused Validation Form *(p.265)*
    - CWE-108: Struts: Unvalidated Action Form *(p.267)*
    - CWE-109: Struts: Validator Turned Off *(p.269)*
    - CWE-110: Struts: Validator Without Form Field *(p.270)*
    - CWE-111: Direct Use of Unsafe JNI *(p.272)*
    - CWE-112: Missing XML Validation *(p.275)*
    - CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.277)*
    - CWE-114: Process Control *(p.283)*
    - CWE-117: Improper Output Neutralization for Logs *(p.294)*
    - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
    - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
    - CWE-134: Use of Externally-Controlled Format String *(p.371)*
    - CWE-15: External Control of System or Configuration Setting *(p.17)*
    - CWE-170: Improper Null Termination *(p.434)*
    - CWE-190: Integer Overflow or Wraparound *(p.478)*
    - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1117)*
    - CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1125)*
    - CWE-73: External Control of File Name or Path *(p.133)*
    - CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer *(p.1664)*

- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.148)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.249)*

CWE-227: 7PK - API Abuse *(p.2334)*
- CWE-242: Use of Inherently Dangerous Function *(p.593)*
- CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.596)*
- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.598)*
- CWE-245: J2EE Bad Practices: Direct Management of Connections *(p.599)*
- CWE-246: J2EE Bad Practices: Direct Use of Sockets *(p.601)*
- CWE-248: Uncaught Exception *(p.603)*
- CWE-250: Execution with Unnecessary Privileges *(p.606)*
- CWE-251: Often Misused: String Management *(p.2335)*
- CWE-252: Unchecked Return Value *(p.613)*
- CWE-558: Use of getlogin() in Multithreaded Application *(p.1281)*

CWE-398: 7PK - Code Quality *(p.2344)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.980)*
- CWE-404: Improper Resource Shutdown or Release *(p.987)*
- CWE-415: Double Free *(p.1015)*
- CWE-416: Use After Free *(p.1019)*
- CWE-457: Use of Uninitialized Variable *(p.1102)*
- CWE-474: Use of Function with Inconsistent Implementations *(p.1136)*
- CWE-475: Undefined Behavior for Input to API *(p.1138)*
- CWE-476: NULL Pointer Dereference *(p.1139)*
- CWE-477: Use of Obsolete Function *(p.1146)*

CWE-485: 7PK - Encapsulation *(p.2349)*
- CWE-486: Comparison of Classes by Name *(p.1172)*
- CWE-488: Exposure of Data Element to Wrong Session *(p.1176)*
- CWE-489: Active Debug Code *(p.1178)*
- CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1181)*
- CWE-492: Use of Inner Class Containing Sensitive Data *(p.1183)*
- CWE-493: Critical Public Variable Without Final Modifier *(p.1190)*
- CWE-495: Private Data Structure Returned From A Public Method *(p.1197)*
- CWE-496: Public Data Assigned to Private Array-Typed Field *(p.1199)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1201)*
- CWE-501: Trust Boundary Violation *(p.1210)*

CWE-2: 7PK - Environment *(p.2329)*
- CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
- CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page *(p.11)*
- CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
- CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
- CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
- CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length *(p.2)*
- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*
- CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote *(p.6)*
- CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*

Graph View: CWE-711: Weaknesses in OWASP Top Ten (2004)

- CWE-722: OWASP Top Ten 2004 Category A1 - Unvalidated Input *(p.2355)*
  - CWE-102: Struts: Duplicate Validation Forms *(p.252)*
  - CWE-103: Struts: Incomplete validate() Method Definition *(p.254)*
  - CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.257)*
  - CWE-106: Struts: Plug-in Framework not in Use *(p.262)*
  - CWE-109: Struts: Validator Turned Off *(p.269)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
  - CWE-166: Improper Handling of Missing Special Element *(p.429)*
  - CWE-167: Improper Handling of Additional Special Element *(p.431)*
  - CWE-179: Incorrect Behavior Order: Early Validation *(p.454)*
  - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.457)*
  - CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.460)*
  - CWE-182: Collapse of Data into Unsafe Value *(p.462)*
  - CWE-183: Permissive List of Allowed Inputs *(p.464)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
  - CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1131)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*
  - CWE-602: Client-Side Enforcement of Server-Side Security *(p.1359)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.148)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
- CWE-723: OWASP Top Ten 2004 Category A2 - Broken Access Control *(p.2356)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-266: Incorrect Privilege Assignment *(p.645)*
  - CWE-268: Privilege Chaining *(p.651)*
  - CWE-275: Permission Issues *(p.2339)*
  - CWE-283: Unverified Ownership *(p.685)*
  - CWE-284: Improper Access Control *(p.687)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-41: Improper Resolution of Path Equivalence *(p.87)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
  - CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1242)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1273)*
  - CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1280)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
  - CWE-708: Incorrect Ownership Assignment *(p.1556)*
  - CWE-73: External Control of File Name or Path *(p.133)*
  - CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*
- CWE-724: OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management *(p.2356)*
  - CWE-255: Credentials Management Errors *(p.2336)*
  - CWE-259: Use of Hard-coded Password *(p.630)*
  - CWE-287: Improper Authentication *(p.699)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.726)*
  - CWE-298: Improper Validation of Certificate Expiration *(p.733)*
  - CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.742)*
  - CWE-304: Missing Critical Step in Authentication *(p.745)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.754)*

- CWE-309: Use of Password System for Primary Authentication *(p.761)*
- CWE-345: Insufficient Verification of Data Authenticity *(p.858)*
- CWE-384: Session Fixation *(p.943)*
- CWE-521: Weak Password Requirements *(p.1231)*
- CWE-522: Insufficiently Protected Credentials *(p.1234)*
- CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1242)*
- CWE-613: Insufficient Session Expiration *(p.1380)*
- CWE-620: Unverified Password Change *(p.1392)*
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1418)*
- CWE-798: Use of Hard-coded Credentials *(p.1699)*

CWE-725: OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws *(p.2357)*
- CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(p.1430)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*

CWE-726: OWASP Top Ten 2004 Category A5 - Buffer Overflows *(p.2358)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
- CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
- CWE-134: Use of Externally-Controlled Format String *(p.371)*

CWE-727: OWASP Top Ten 2004 Category A6 - Injection Flaws *(p.2358)*
- CWE-117: Improper Output Neutralization for Logs *(p.294)*
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.138)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.148)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.220)*
- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.232)*
- CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.242)*

CWE-728: OWASP Top Ten 2004 Category A7 - Improper Error Handling *(p.2359)*
- CWE-203: Observable Discrepancy *(p.525)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.575)*
- CWE-252: Unchecked Return Value *(p.613)*
- CWE-389: Error Conditions, Return Values, Status Codes *(p.2344)*
- CWE-390: Detection of Error Condition Without Action *(p.950)*
- CWE-391: Unchecked Error Condition *(p.955)*
- CWE-394: Unexpected Status Code or Return Value *(p.962)*
- CWE-636: Not Failing Securely ('Failing Open') *(p.1409)*
- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*

CWE-729: OWASP Top Ten 2004 Category A8 - Insecure Storage *(p.2359)*
- CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.569)*
- CWE-261: Weak Encoding for Password *(p.638)*
- CWE-311: Missing Encryption of Sensitive Data *(p.764)*
- CWE-321: Use of Hard-coded Cryptographic Key *(p.792)*
- CWE-326: Inadequate Encryption Strength *(p.803)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
- CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1259)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1338)*
- CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1349)*

CWE-730: OWASP Top Ten 2004 Category A9 - Denial of Service *(p.2360)*
- CWE-170: Improper Null Termination *(p.434)*
- CWE-248: Uncaught Exception *(p.603)*

- CWE-369: Divide By Zero *(p.920)*
- CWE-382: J2EE Bad Practices: Use of System.exit() *(p.940)*
- CWE-400: Uncontrolled Resource Consumption *(p.971)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.980)*
- CWE-404: Improper Resource Shutdown or Release *(p.987)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.993)*
- CWE-410: Insufficient Resource Pool *(p.1005)*
- CWE-412: Unrestricted Externally Accessible Lock *(p.1007)*
- CWE-476: NULL Pointer Dereference *(p.1139)*
- CWE-674: Uncontrolled Recursion *(p.1493)*

CWE-731: OWASP Top Ten 2004 Category A10 - Insecure Configuration Management *(p.2360)*

- CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
- CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.558)*
- CWE-219: Storage of File with Sensitive Data Under Web Root *(p.560)*
- CWE-275: Permission Issues *(p.2339)*
- CWE-295: Improper Certificate Validation *(p.721)*
- CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
- CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1279)*
- CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length *(p.2)*
- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*
- CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote *(p.6)*
- CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*
- CWE-459: Incomplete Cleanup *(p.1106)*
- CWE-489: Active Debug Code *(p.1178)*
- CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
- CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page *(p.11)*
- CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
- CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1230)*
- CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework *(p.1278)*
- CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1280)*
- CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1243)*
- CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1245)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1246)*
- CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1247)*
- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1248)*
- CWE-531: Inclusion of Sensitive Information in Test Code *(p.1249)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1250)*
- CWE-540: Inclusion of Sensitive Information in Source Code *(p.1260)*
- CWE-541: Inclusion of Sensitive Information in an Include File *(p.1262)*
- CWE-548: Exposure of Information Through Directory Listing *(p.1269)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1274)*

Graph View: CWE-734: Weaknesses Addressed by the CERT C Secure Coding Standard (2008)

- CWE-735: CERT C Secure Coding Standard (2008) Chapter 2 - Preprocessor (PRE) *(p.2361)*
  - CWE-684: Incorrect Provision of Specified Functionality *(p.1514)*
- CWE-736: CERT C Secure Coding Standard (2008) Chapter 3 - Declarations and Initialization (DCL) *(p.2362)*
  - CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1267)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1407)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
- CWE-737: CERT C Secure Coding Standard (2008) Chapter 4 - Expressions (EXP) *(p.2362)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1118)*
  - CWE-468: Incorrect Pointer Scaling *(p.1121)*
  - CWE-476: NULL Pointer Dereference *(p.1139)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1407)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1547)*
  - CWE-783: Operator Precedence Logic Error *(p.1659)*
- CWE-738: CERT C Secure Coding Standard (2008) Chapter 5 - Integers (INT) *(p.2363)*
  - CWE-129: Improper Validation of Array Index *(p.347)*
  - CWE-190: Integer Overflow or Wraparound *(p.478)*
  - CWE-192: Integer Coercion Error *(p.489)*
  - CWE-197: Numeric Truncation Error *(p.507)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-369: Divide By Zero *(p.920)*
  - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1117)*
  - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1330)*
  - CWE-606: Unchecked Input for Loop Condition *(p.1366)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1498)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
  - CWE-682: Incorrect Calculation *(p.1507)*
- CWE-739: CERT C Secure Coding Standard (2008) Chapter 6 - Floating Point (FLP) *(p.2364)*
  - CWE-369: Divide By Zero *(p.920)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
  - CWE-682: Incorrect Calculation *(p.1507)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
- CWE-740: CERT C Secure Coding Standard (2008) Chapter 7 - Arrays (ARR) *(p.2365)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-129: Improper Validation of Array Index *(p.347)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1118)*
  - CWE-469: Use of Pointer Subtraction to Determine Size *(p.1123)*
  - CWE-665: Improper Initialization *(p.1465)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1711)*
- CWE-741: CERT C Secure Coding Standard (2008) Chapter 8 - Characters and Strings (STR) *(p.2366)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
  - CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.377)*
  - CWE-170: Improper Null Termination *(p.434)*
  - CWE-193: Off-by-one Error *(p.493)*
  - CWE-464: Addition of Data Structure Sentinel *(p.1115)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1547)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*
- CWE-742: CERT C Secure Coding Standard (2008) Chapter 9 - Memory Management (MEM) *(p.2367)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
- CWE-128: Wrap-around Error *(p.345)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.361)*
- CWE-190: Integer Overflow or Wraparound *(p.478)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.569)*
- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.598)*
- CWE-252: Unchecked Return Value *(p.613)*
- CWE-415: Double Free *(p.1015)*
- CWE-416: Use After Free *(p.1019)*
- CWE-476: NULL Pointer Dereference *(p.1139)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1246)*
- CWE-590: Free of Memory not on the Heap *(p.1335)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1338)*
- CWE-628: Function Call with Incorrectly Specified Arguments *(p.1407)*
- CWE-665: Improper Initialization *(p.1465)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1518)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1577)*

CWE-743: CERT C Secure Coding Standard (2008) Chapter 10 - Input Output (FIO) *(p.2368)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
- CWE-134: Use of Externally-Controlled Format String *(p.371)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.591)*
- CWE-276: Incorrect Default Permissions *(p.672)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.678)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.913)*
- CWE-37: Path Traversal: '/absolute/pathname/here' *(p.79)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.937)*
- CWE-38: Path Traversal: '\absolute\pathname\here' *(p.81)*
- CWE-39: Path Traversal: 'C:dirname' *(p.83)*
- CWE-391: Unchecked Error Condition *(p.955)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.985)*
- CWE-404: Improper Resource Shutdown or Release *(p.987)*
- CWE-41: Improper Resolution of Path Equivalence *(p.87)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1274)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.112)*
- CWE-62: UNIX Hard Link *(p.120)*
- CWE-64: Windows Shortcut Following (.LNK) *(p.122)*
- CWE-65: Windows Hard Link *(p.124)*
- CWE-67: Improper Handling of Windows Device Names *(p.127)*
- CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1496)*
- CWE-676: Use of Potentially Dangerous Function *(p.1498)*
- CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*

CWE-744: CERT C Secure Coding Standard (2008) Chapter 11 - Environment (ENV) *(p.2369)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
- CWE-426: Untrusted Search Path *(p.1035)*
- CWE-462: Duplicate Key in Associative List (Alist) *(p.1111)*
- CWE-705: Incorrect Control Flow Scoping *(p.1550)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*

- CWE-745: CERT C Secure Coding Standard (2008) Chapter 12 - Signals (SIG) *(p.2370)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1154)*
  - CWE-662: Improper Synchronization *(p.1457)*
- CWE-746: CERT C Secure Coding Standard (2008) Chapter 13 - Error Handling (ERR) *(p.2371)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-391: Unchecked Error Condition *(p.955)*
  - CWE-544: Missing Standardized Error Handling Mechanism *(p.1265)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1498)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1550)*
- CWE-747: CERT C Secure Coding Standard (2008) Chapter 14 - Miscellaneous (MSC) *(p.2371)*
  - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
  - CWE-176: Improper Handling of Unicode Encoding *(p.446)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-480: Use of Incorrect Operator *(p.1157)*
  - CWE-482: Comparing instead of Assigning *(p.1165)*
  - CWE-561: Dead Code *(p.1283)*
  - CWE-563: Assignment to Variable without Use *(p.1289)*
  - CWE-570: Expression is Always False *(p.1300)*
  - CWE-571: Expression is Always True *(p.1303)*
  - CWE-697: Incorrect Comparison *(p.1538)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1547)*
- CWE-748: CERT C Secure Coding Standard (2008) Appendix - POSIX (POS) *(p.2372)*
  - CWE-170: Improper Null Termination *(p.434)*
  - CWE-242: Use of Inherently Dangerous Function *(p.593)*
  - CWE-272: Least Privilege Violation *(p.663)*
  - CWE-273: Improper Check for Dropped Privileges *(p.667)*
  - CWE-363: Race Condition Enabling Link Following *(p.904)*
  - CWE-366: Race Condition within a Thread *(p.910)*
  - CWE-562: Return of Stack Variable Address *(p.1287)*
  - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.112)*
  - CWE-667: Improper Locking *(p.1472)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
  - CWE-696: Incorrect Behavior Order *(p.1535)*

Graph View: CWE-750: Weaknesses in the 2009 CWE/ SANS Top 25 Most Dangerous Programming Errors

- CWE-751: 2009 Top 25 - Insecure Interaction Between Components *(p.2373)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.287)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.875)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
- CWE-752: 2009 Top 25 - Risky Resource Management *(p.2374)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-404: Improper Resource Shutdown or Release *(p.987)*
  - CWE-426: Untrusted Search Path *(p.1035)*
  - CWE-494: Download of Code Without Integrity Check *(p.1192)*
  - CWE-642: External Control of Critical State Data *(p.1422)*
  - CWE-665: Improper Initialization *(p.1465)*
  - CWE-682: Incorrect Calculation *(p.1507)*
  - CWE-73: External Control of File Name or Path *(p.133)*
  - CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.225)*
- CWE-753: 2009 Top 25 - Porous Defenses *(p.2374)*
  - CWE-250: Execution with Unnecessary Privileges *(p.606)*
  - CWE-259: Use of Hard-coded Password *(p.630)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-602: Client-Side Enforcement of Server-Side Security *(p.1359)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
  - CWE-798: Use of Hard-coded Credentials *(p.1699)*

Graph View: CWE-800: Weaknesses in the 2010 CWE/ SANS Top 25 Most Dangerous Programming Errors

- CWE-808: 2010 Top 25 - Weaknesses On the Cusp *(p.2376)*
  - CWE-134: Use of Externally-Controlled Format String *(p.371)*
  - CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.551)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.754)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-416: Use After Free *(p.1019)*
  - CWE-426: Untrusted Search Path *(p.1035)*
  - CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1092)*
  - CWE-456: Missing Initialization of a Variable *(p.1096)*
  - CWE-476: NULL Pointer Dereference *(p.1139)*
  - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.112)*
  - CWE-672: Operation on a Resource after Expiration or Release *(p.1488)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
  - CWE-749: Exposed Dangerous Method or Function *(p.1572)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1632)*
  - CWE-799: Improper Control of Interaction Frequency *(p.1708)*
  - CWE-804: Guessable CAPTCHA *(p.1710)*
- CWE-803: 2010 Top 25 - Porous Defenses *(p.2376)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-306: Missing Authentication for Critical Function *(p.748)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
  - CWE-798: Use of Hard-coded Credentials *(p.1699)*
  - CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1723)*
- CWE-802: 2010 Top 25 - Risky Resource Management *(p.2375)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
  - CWE-129: Improper Validation of Array Index *(p.347)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.361)*
  - CWE-190: Integer Overflow or Wraparound *(p.478)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-494: Download of Code Without Integrity Check *(p.1192)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1577)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1711)*
  - CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.242)*
- CWE-801: 2010 Top 25 - Insecure Interaction Between Components *(p.2375)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.875)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1055)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*

Graph View: CWE-809: Weaknesses in OWASP Top Ten (2010)

- CWE-810: OWASP Top Ten 2010 Category A1 - Injection *(p.2377)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.217)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.220)*
- CWE-811: OWASP Top Ten 2010 Category A2 - Cross-Site Scripting (XSS) *(p.2378)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
- CWE-812: OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management *(p.2378)*
  - CWE-287: Improper Authentication *(p.699)*
  - CWE-306: Missing Authentication for Critical Function *(p.748)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.754)*
  - CWE-798: Use of Hard-coded Credentials *(p.1699)*
- CWE-813: OWASP Top Ten 2010 Category A4 - Insecure Direct Object References *(p.2378)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1055)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
  - CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1750)*
  - CWE-862: Missing Authorization *(p.1789)*
  - CWE-863: Incorrect Authorization *(p.1796)*
  - CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.249)*
- CWE-814: OWASP Top Ten 2010 Category A5 - Cross-Site Request Forgery(CSRF) *(p.2379)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.875)*
- CWE-815: OWASP Top Ten 2010 Category A6 - Security Misconfiguration *(p.2379)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.560)*
  - CWE-250: Execution with Unnecessary Privileges *(p.606)*
  - CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1257)*
  - CWE-552: Files or Directories Accessible to External Parties *(p.1274)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
- CWE-816: OWASP Top Ten 2010 Category A7 - Insecure Cryptographic Storage *(p.2380)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.771)*
  - CWE-326: Inadequate Encryption Strength *(p.803)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-759: Use of a One-Way Hash without a Salt *(p.1593)*
- CWE-817: OWASP Top Ten 2010 Category A8 - Failure to Restrict URL Access *(p.2380)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-862: Missing Authorization *(p.1789)*
  - CWE-863: Incorrect Authorization *(p.1796)*
- CWE-818: OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection *(p.2381)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
- CWE-819: OWASP Top Ten 2010 Category A10 - Unvalidated Redirects and Forwards *(p.2381)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*

Graph View: CWE-844: Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)

- CWE-845: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 2 - Input Validation and Data Sanitization (IDS) *(p.2383)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.287)*
  - CWE-134: Use of Externally-Controlled Format String *(p.371)*
  - CWE-144: Improper Neutralization of Line Delimiters *(p.389)*
  - CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences *(p.400)*
  - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.457)*
  - CWE-182: Collapse of Data into Unsafe Value *(p.462)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.710)*
  - CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.1004)*
  - CWE-625: Permissive Regular Expression *(p.1400)*
  - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1435)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-838: Inappropriate Encoding for Output Context *(p.1773)*
- CWE-846: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 3 - Declarations and Initialization (DCL) *(p.2383)*
  - CWE-665: Improper Initialization *(p.1465)*
- CWE-847: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 4 - Expressions (EXP) *(p.2384)*
  - CWE-252: Unchecked Return Value *(p.613)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1154)*
  - CWE-595: Comparison of Object References Instead of Object Contents *(p.1342)*
  - CWE-597: Use of Wrong Operator in String Comparison *(p.1345)*
- CWE-848: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 5 - Numeric Types and Operations (NUM) *(p.2384)*
  - CWE-197: Numeric Truncation Error *(p.507)*
  - CWE-369: Divide By Zero *(p.920)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
- CWE-849: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 6 - Object Orientation (OBJ) *(p.2385)*
  - CWE-374: Passing Mutable Objects to an Untrusted Method *(p.927)*
  - CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.930)*
  - CWE-486: Comparison of Classes by Name *(p.1172)*
  - CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1181)*
  - CWE-492: Use of Inner Class Containing Sensitive Data *(p.1183)*
  - CWE-493: Critical Public Variable Without Final Modifier *(p.1190)*
  - CWE-498: Cloneable Class Containing Sensitive Information *(p.1204)*
  - CWE-500: Public Static Field Not Marked Final *(p.1208)*
  - CWE-582: Array Declared Public, Final, and Static *(p.1322)*
  - CWE-766: Critical Data Element Declared Public *(p.1615)*
- CWE-850: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 7 - Methods (MET) *(p.2385)*
  - CWE-487: Reliance on Package-level Scope *(p.1175)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1299)*
  - CWE-573: Improper Following of Specification by Caller *(p.1307)*
  - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1321)*
  - CWE-583: finalize() Method Declared Public *(p.1324)*
  - CWE-586: Explicit Call to Finalize() *(p.1329)*
  - CWE-589: Call to Non-ubiquitous API *(p.1333)*
  - CWE-617: Reachable Assertion *(p.1387)*
- CWE-851: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 8 - Exceptional Behavior (ERR) *(p.2386)*

- CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
- CWE-230: Improper Handling of Missing Values *(p.578)*
- CWE-232: Improper Handling of Undefined Values *(p.580)*
- CWE-248: Uncaught Exception *(p.603)*
- CWE-382: J2EE Bad Practices: Use of System.exit() *(p.940)*
- CWE-390: Detection of Error Condition Without Action *(p.950)*
- CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.964)*
- CWE-397: Declaration of Throws for Generic Exception *(p.968)*
- CWE-460: Improper Cleanup on Thrown Exception *(p.1109)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1201)*
- CWE-584: Return Inside Finally Block *(p.1325)*
- CWE-600: Uncaught Exception in Servlet *(p.1352)*
- CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1523)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1544)*
- CWE-705: Incorrect Control Flow Scoping *(p.1550)*

CWE-852: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 9 - Visibility and Atomicity (VNA) *(p.2387)*

- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
- CWE-366: Race Condition within a Thread *(p.910)*
- CWE-413: Improper Resource Locking *(p.1010)*
- CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1296)*
- CWE-662: Improper Synchronization *(p.1457)*
- CWE-667: Improper Locking *(p.1472)*

CWE-853: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 10 - Locking (LCK) *(p.2387)*

- CWE-412: Unrestricted Externally Accessible Lock *(p.1007)*
- CWE-413: Improper Resource Locking *(p.1010)*
- CWE-609: Double-Checked Locking *(p.1371)*
- CWE-667: Improper Locking *(p.1472)*
- CWE-820: Missing Synchronization *(p.1729)*
- CWE-833: Deadlock *(p.1762)*

CWE-854: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 11 - Thread APIs (THI) *(p.2388)*

- CWE-572: Call to Thread run() instead of start() *(p.1305)*
- CWE-705: Incorrect Control Flow Scoping *(p.1550)*

CWE-855: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 12 - Thread Pools (TPS) *(p.2388)*

- CWE-392: Missing Report of Error Condition *(p.958)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.993)*
- CWE-410: Insufficient Resource Pool *(p.1005)*

CWE-856: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 13 - Thread-Safety Miscellaneous (TSM) *(p.2389)*

CWE-857: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 14 - Input Output (FIO) *(p.2389)*

- CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.377)*
- CWE-198: Use of Incorrect Byte Ordering *(p.510)*
- CWE-276: Incorrect Default Permissions *(p.672)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.678)*
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.889)*
- CWE-377: Insecure Temporary File *(p.932)*
- CWE-404: Improper Resource Shutdown or Release *(p.987)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.993)*
- CWE-459: Incomplete Cleanup *(p.1106)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1250)*
- CWE-67: Improper Handling of Windows Device Names *(p.127)*

- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*

CWE-858: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 15 - Serialization (SER) *(p.2390)*

- CWE-250: Execution with Unnecessary Privileges *(p.606)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
- CWE-400: Uncontrolled Resource Consumption *(p.971)*
- CWE-499: Serializable Class Containing Sensitive Data *(p.1206)*
- CWE-502: Deserialization of Untrusted Data *(p.1212)*
- CWE-589: Call to Non-ubiquitous API *(p.1333)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*

CWE-859: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 16 - Platform Security (SEC) *(p.2390)*

- CWE-111: Direct Use of Unsafe JNI *(p.272)*
- CWE-266: Incorrect Privilege Assignment *(p.645)*
- CWE-272: Least Privilege Violation *(p.663)*
- CWE-300: Channel Accessible by Non-Endpoint *(p.737)*
- CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.742)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.864)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1125)*
- CWE-494: Download of Code Without Integrity Check *(p.1192)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1723)*

CWE-860: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 17 - Runtime Environment (ENV) *(p.2391)*

- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.868)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*

CWE-861: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 18 - Miscellaneous (MSC) *(p.2391)*

- CWE-259: Use of Hard-coded Password *(p.630)*
- CWE-311: Missing Encryption of Sensitive Data *(p.764)*
- CWE-330: Use of Insufficiently Random Values *(p.821)*
- CWE-332: Insufficient Entropy in PRNG *(p.830)*
- CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.832)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.839)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.841)*
- CWE-400: Uncontrolled Resource Consumption *(p.971)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.980)*
- CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1263)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*
- CWE-798: Use of Hard-coded Credentials *(p.1699)*

Graph View: CWE-868: Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version)

- CWE-869: CERT C++ Secure Coding Section 01 - Preprocessor (PRE) *(p.2394)*
- CWE-870: CERT C++ Secure Coding Section 02 - Declarations and Initialization (DCL) *(p.2395)*
- CWE-871: CERT C++ Secure Coding Section 03 - Expressions (EXP) *(p.2395)*
  - CWE-476: NULL Pointer Dereference *(p.1139)*
  - CWE-480: Use of Incorrect Operator *(p.1157)*
  - CWE-768: Incorrect Short Circuit Evaluation *(p.1620)*
- CWE-872: CERT C++ Secure Coding Section 04 - Integers (INT) *(p.2395)*
  - CWE-129: Improper Validation of Array Index *(p.347)*
  - CWE-190: Integer Overflow or Wraparound *(p.478)*
  - CWE-192: Integer Coercion Error *(p.489)*
  - CWE-197: Numeric Truncation Error *(p.507)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-369: Divide By Zero *(p.920)*
  - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1117)*
  - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1330)*
  - CWE-606: Unchecked Input for Loop Condition *(p.1366)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1498)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
  - CWE-682: Incorrect Calculation *(p.1507)*
- CWE-873: CERT C++ Secure Coding Section 05 - Floating Point Arithmetic (FLP) *(p.2396)*
  - CWE-369: Divide By Zero *(p.920)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
  - CWE-682: Incorrect Calculation *(p.1507)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
- CWE-874: CERT C++ Secure Coding Section 06 - Arrays and the STL (ARR) *(p.2396)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-129: Improper Validation of Array Index *(p.347)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1118)*
  - CWE-469: Use of Pointer Subtraction to Determine Size *(p.1123)*
  - CWE-665: Improper Initialization *(p.1465)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1711)*
- CWE-875: CERT C++ Secure Coding Section 07 - Characters and Strings (STR) *(p.2397)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
  - CWE-170: Improper Null Termination *(p.434)*
  - CWE-193: Off-by-one Error *(p.493)*
  - CWE-464: Addition of Data Structure Sentinel *(p.1115)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1547)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*
- CWE-876: CERT C++ Secure Coding Section 08 - Memory Management (MEM) *(p.2398)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-128: Wrap-around Error *(p.345)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.361)*
  - CWE-190: Integer Overflow or Wraparound *(p.478)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.569)*
  - CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.598)*
  - CWE-252: Unchecked Return Value *(p.613)*

- CWE-391: Unchecked Error Condition *(p.955)*
- CWE-404: Improper Resource Shutdown or Release *(p.987)*
- CWE-415: Double Free *(p.1015)*
- CWE-416: Use After Free *(p.1019)*
- CWE-476: NULL Pointer Dereference *(p.1139)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1246)*
- CWE-590: Free of Memory not on the Heap *(p.1335)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1338)*
- CWE-665: Improper Initialization *(p.1465)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1518)*
- CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1523)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1544)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1577)*
- CWE-762: Mismatched Memory Management Routines *(p.1605)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*
- CWE-822: Untrusted Pointer Dereference *(p.1732)*

CWE-877: CERT C++ Secure Coding Section 09 - Input Output (FIO) *(p.2398)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
- CWE-134: Use of Externally-Controlled Format String *(p.371)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.591)*
- CWE-276: Incorrect Default Permissions *(p.672)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.678)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.913)*
- CWE-37: Path Traversal: '/absolute/pathname/here' *(p.79)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.937)*
- CWE-38: Path Traversal: '\absolute\pathname\here' *(p.81)*
- CWE-39: Path Traversal: 'C:dirname' *(p.83)*
- CWE-391: Unchecked Error Condition *(p.955)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.985)*
- CWE-404: Improper Resource Shutdown or Release *(p.987)*
- CWE-41: Improper Resolution of Path Equivalence *(p.87)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1274)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.112)*
- CWE-62: UNIX Hard Link *(p.120)*
- CWE-64: Windows Shortcut Following (.LNK) *(p.122)*
- CWE-65: Windows Hard Link *(p.124)*
- CWE-67: Improper Handling of Windows Device Names *(p.127)*
- CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1496)*
- CWE-676: Use of Potentially Dangerous Function *(p.1498)*
- CWE-73: External Control of File Name or Path *(p.133)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*

CWE-878: CERT C++ Secure Coding Section 10 - Environment (ENV) *(p.2399)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
- CWE-426: Untrusted Search Path *(p.1035)*
- CWE-462: Duplicate Key in Associative List (Alist) *(p.1111)*
- CWE-705: Incorrect Control Flow Scoping *(p.1550)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1723)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*

- CWE-879: CERT C++ Secure Coding Section 11 - Signals (SIG) *(p.2400)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1154)*
  - CWE-662: Improper Synchronization *(p.1457)*
- CWE-880: CERT C++ Secure Coding Section 12 - Exceptions and Error Handling (ERR) *(p.2400)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-390: Detection of Error Condition Without Action *(p.950)*
  - CWE-391: Unchecked Error Condition *(p.955)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1109)*
  - CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1201)*
  - CWE-544: Missing Standardized Error Handling Mechanism *(p.1265)*
  - CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1544)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1550)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1577)*
  - CWE-755: Improper Handling of Exceptional Conditions *(p.1585)*
- CWE-881: CERT C++ Secure Coding Section 13 - Object Oriented Programming (OOP) *(p.2401)*
- CWE-882: CERT C++ Secure Coding Section 14 - Concurrency (CON) *(p.2401)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
  - CWE-366: Race Condition within a Thread *(p.910)*
  - CWE-404: Improper Resource Shutdown or Release *(p.987)*
  - CWE-488: Exposure of Data Element to Wrong Session *(p.1176)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1632)*
- CWE-883: CERT C++ Secure Coding Section 49 - Miscellaneous (MSC) *(p.2402)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.287)*
  - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
  - CWE-176: Improper Handling of Unicode Encoding *(p.446)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-480: Use of Incorrect Operator *(p.1157)*
  - CWE-482: Comparing instead of Assigning *(p.1165)*
  - CWE-561: Dead Code *(p.1283)*
  - CWE-563: Assignment to Variable without Use *(p.1289)*
  - CWE-570: Expression is Always False *(p.1300)*
  - CWE-571: Expression is Always True *(p.1303)*
  - CWE-697: Incorrect Comparison *(p.1538)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1547)*

Graph View: CWE-888: Software Fault Pattern (SFP) Clusters

- CWE-885: SFP Primary Cluster: Risky Values *(p.2403)*
  - CWE-998: SFP Secondary Cluster: Glitch in Computation *(p.2440)*
    - CWE-128: Wrap-around Error *(p.345)*
    - CWE-190: Integer Overflow or Wraparound *(p.478)*
    - CWE-191: Integer Underflow (Wrap or Wraparound) *(p.487)*
    - CWE-194: Unexpected Sign Extension *(p.498)*
    - CWE-195: Signed to Unsigned Conversion Error *(p.501)*
    - CWE-196: Unsigned to Signed Conversion Error *(p.505)*
    - CWE-197: Numeric Truncation Error *(p.507)*
    - CWE-369: Divide By Zero *(p.920)*
    - CWE-456: Missing Initialization of a Variable *(p.1096)*
    - CWE-457: Use of Uninitialized Variable *(p.1102)*
    - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1117)*
    - CWE-468: Incorrect Pointer Scaling *(p.1121)*
    - CWE-475: Undefined Behavior for Input to API *(p.1138)*
    - CWE-480: Use of Incorrect Operator *(p.1157)*
    - CWE-481: Assigning instead of Comparing *(p.1161)*
    - CWE-486: Comparison of Classes by Name *(p.1172)*
    - CWE-562: Return of Stack Variable Address *(p.1287)*
    - CWE-570: Expression is Always False *(p.1300)*
    - CWE-571: Expression is Always True *(p.1303)*
    - CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session *(p.1318)*
    - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1330)*
    - CWE-594: J2EE Framework: Saving Unserializable Objects to Disk *(p.1341)*
    - CWE-597: Use of Wrong Operator in String Comparison *(p.1345)*
    - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1407)*
    - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
    - CWE-683: Function Call With Incorrect Order of Arguments *(p.1512)*
    - CWE-685: Function Call With Incorrect Number of Arguments *(p.1516)*
    - CWE-686: Function Call With Incorrect Argument Type *(p.1517)*
    - CWE-688: Function Call With Incorrect Variable or Reference as Argument *(p.1520)*
    - CWE-704: Incorrect Type Conversion or Cast *(p.1547)*
    - CWE-768: Incorrect Short Circuit Evaluation *(p.1620)*
- CWE-886: SFP Primary Cluster: Unused entities *(p.2403)*
  - CWE-482: Comparing instead of Assigning *(p.1165)*
  - CWE-561: Dead Code *(p.1283)*
  - CWE-563: Assignment to Variable without Use *(p.1289)*
- CWE-887: SFP Primary Cluster: API *(p.2403)*
  - CWE-1001: SFP Secondary Cluster: Use of an Improper API *(p.2441)*
    - CWE-111: Direct Use of Unsafe JNI *(p.272)*
    - CWE-227: 7PK - API Abuse *(p.2334)*
    - CWE-242: Use of Inherently Dangerous Function *(p.593)*
    - CWE-245: J2EE Bad Practices: Direct Management of Connections *(p.599)*
    - CWE-246: J2EE Bad Practices: Direct Use of Sockets *(p.601)*
    - CWE-382: J2EE Bad Practices: Use of System.exit() *(p.940)*
    - CWE-383: J2EE Bad Practices: Direct Use of Threads *(p.942)*
    - CWE-432: Dangerous Signal Handler not Disabled During Sensitive Operations *(p.1052)*
    - CWE-439: Behavioral Change in New Version or Environment *(p.1068)*
    - CWE-440: Expected Behavior Violation *(p.1069)*
    - CWE-474: Use of Function with Inconsistent Implementations *(p.1136)*
    - CWE-477: Use of Obsolete Function *(p.1146)*

- CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1154)*
- CWE-558: Use of getlogin() in Multithreaded Application *(p.1281)*
- CWE-572: Call to Thread run() instead of start() *(p.1305)*
- CWE-573: Improper Following of Specification by Caller *(p.1307)*
- CWE-574: EJB Bad Practices: Use of Synchronization Primitives *(p.1308)*
- CWE-575: EJB Bad Practices: Use of AWT Swing *(p.1310)*
- CWE-576: EJB Bad Practices: Use of Java I/O *(p.1312)*
- CWE-577: EJB Bad Practices: Use of Sockets *(p.1314)*
- CWE-578: EJB Bad Practices: Use of Class Loader *(p.1316)*
- CWE-586: Explicit Call to Finalize() *(p.1329)*
- CWE-589: Call to Non-ubiquitous API *(p.1333)*
- CWE-617: Reachable Assertion *(p.1387)*
- CWE-676: Use of Potentially Dangerous Function *(p.1498)*
- CWE-684: Incorrect Provision of Specified Functionality *(p.1514)*
- CWE-695: Use of Low-Level Functionality *(p.1533)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1591)*

CWE-889: SFP Primary Cluster: Exception Management *(p.2403)*

- CWE-960: SFP Secondary Cluster: Ambiguous Exception Type *(p.2420)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.966)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.968)*
- CWE-961: SFP Secondary Cluster: Incorrect Exception Behavior *(p.2420)*
  - CWE-392: Missing Report of Error Condition *(p.958)*
  - CWE-393: Return of Wrong Status Code *(p.960)*
  - CWE-455: Non-exit on Failed Initialization *(p.1095)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1109)*
  - CWE-544: Missing Standardized Error Handling Mechanism *(p.1265)*
  - CWE-584: Return Inside Finally Block *(p.1325)*
  - CWE-636: Not Failing Securely ('Failing Open') *(p.1409)*
  - CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1544)*
- CWE-962: SFP Secondary Cluster: Unchecked Status Condition *(p.2421)*
  - CWE-248: Uncaught Exception *(p.603)*
  - CWE-252: Unchecked Return Value *(p.613)*
  - CWE-253: Incorrect Check of Function Return Value *(p.620)*
  - CWE-273: Improper Check for Dropped Privileges *(p.667)*
  - CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.679)*
  - CWE-372: Incomplete Internal State Distinction *(p.926)*
  - CWE-390: Detection of Error Condition Without Action *(p.950)*
  - CWE-391: Unchecked Error Condition *(p.955)*
  - CWE-394: Unexpected Status Code or Return Value *(p.962)*
  - CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.964)*
  - CWE-431: Missing Handler *(p.1051)*
  - CWE-478: Missing Default Case in Multiple Condition Expression *(p.1149)*
  - CWE-484: Omitted Break Statement in Switch *(p.1169)*
  - CWE-600: Uncaught Exception in Servlet *(p.1352)*
  - CWE-665: Improper Initialization *(p.1465)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1577)*
  - CWE-755: Improper Handling of Exceptional Conditions *(p.1585)*

CWE-890: SFP Primary Cluster: Memory Access *(p.2404)*

- CWE-970: SFP Secondary Cluster: Faulty Buffer Access *(p.2426)*
  - CWE-118: Incorrect Access of Indexable Resource ('Range Error') *(p.298)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.299)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
  - CWE-121: Stack-based Buffer Overflow *(p.320)*
  - CWE-122: Heap-based Buffer Overflow *(p.324)*

- CWE-65: Windows Hard Link *(p.124)*

- CWE-981: SFP Secondary Cluster: Path Traversal *(p.2430)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-23: Relative Path Traversal *(p.46)*
  - CWE-24: Path Traversal: '../filedir' *(p.53)*
  - CWE-25: Path Traversal: '/../filedir' *(p.55)*
  - CWE-26: Path Traversal: '/dir/../filename' *(p.57)*
  - CWE-27: Path Traversal: 'dir/../../filename' *(p.58)*
  - CWE-28: Path Traversal: '..\filedir' *(p.60)*
  - CWE-29: Path Traversal: '\..\filename' *(p.62)*
  - CWE-30: Path Traversal: '\dir\..\filename' *(p.64)*
  - CWE-31: Path Traversal: 'dir\..\..\filename' *(p.65)*
  - CWE-32: Path Traversal: '...' (Triple Dot) *(p.67)*
  - CWE-33: Path Traversal: '....' (Multiple Dot) *(p.69)*
  - CWE-34: Path Traversal: '..../' *(p.71)*
  - CWE-35: Path Traversal: '.../.../' *(p.73)*
  - CWE-36: Absolute Path Traversal *(p.75)*
  - CWE-37: Path Traversal: '/absolute/pathname/here' *(p.79)*
  - CWE-38: Path Traversal: '\absolute\pathname\here' *(p.81)*
  - CWE-39: Path Traversal: 'C:dirname' *(p.83)*
  - CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) *(p.86)*
  - CWE-41: Improper Resolution of Path Equivalence *(p.87)*
  - CWE-42: Path Equivalence: 'filename.' (Trailing Dot) *(p.93)*
  - CWE-428: Unquoted Search Path or Element *(p.1047)*
  - CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) *(p.94)*
  - CWE-44: Path Equivalence: 'file.name' (Internal Dot) *(p.95)*
  - CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) *(p.96)*
  - CWE-46: Path Equivalence: 'filename ' (Trailing Space) *(p.97)*
  - CWE-47: Path Equivalence: ' filename' (Leading Space) *(p.98)*
  - CWE-48: Path Equivalence: 'file name' (Internal Whitespace) *(p.99)*
  - CWE-49: Path Equivalence: 'filename/' (Trailing Slash) *(p.100)*
  - CWE-50: Path Equivalence: '//multiple/leading/slash' *(p.101)*
  - CWE-51: Path Equivalence: '/multiple//internal/slash' *(p.103)*
  - CWE-52: Path Equivalence: '/multiple/trailing/slash//' *(p.104)*
  - CWE-53: Path Equivalence: '\multiple\\internal\backslash' *(p.105)*
  - CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) *(p.106)*
  - CWE-55: Path Equivalence: '/./' (Single Dot Directory) *(p.107)*
  - CWE-56: Path Equivalence: 'filedir*' (Wildcard) *(p.108)*
  - CWE-57: Path Equivalence: 'fakedir/../realdir/filename' *(p.109)*
  - CWE-58: Path Equivalence: Windows 8.3 Filename *(p.111)*
  - CWE-66: Improper Handling of File Names that Identify Virtual Resources *(p.125)*
  - CWE-67: Improper Handling of Windows Device Names *(p.127)*
  - CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1553)*
  - CWE-72: Improper Handling of Apple HFS+ Alternate Data Stream Path *(p.131)*
  - CWE-73: External Control of File Name or Path *(p.133)*

- CWE-894: SFP Primary Cluster: Synchronization *(p.2405)*
  - CWE-986: SFP Secondary Cluster: Missing Lock *(p.2432)*
    - CWE-364: Signal Handler Race Condition *(p.905)*
    - CWE-366: Race Condition within a Thread *(p.910)*
    - CWE-368: Context Switching Race Condition *(p.918)*
    - CWE-413: Improper Resource Locking *(p.1010)*
    - CWE-414: Missing Lock Check *(p.1014)*
    - CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1263)*
    - CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1296)*

- CWE-609: Double-Checked Locking *(p.1371)*
- CWE-662: Improper Synchronization *(p.1457)*
- CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1461)*
- CWE-667: Improper Locking *(p.1472)*

- CWE-987: SFP Secondary Cluster: Multiple Locks/Unlocks *(p.2433)*
  - CWE-585: Empty Synchronized Block *(p.1327)*
  - CWE-764: Multiple Locks of a Critical Resource *(p.1613)*
  - CWE-765: Multiple Unlocks of a Critical Resource *(p.1614)*
- CWE-988: SFP Secondary Cluster: Race Condition Window *(p.2433)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
  - CWE-363: Race Condition Enabling Link Following *(p.904)*
  - CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.913)*
  - CWE-370: Missing Check for Certificate Revocation after Initial Check *(p.924)*
  - CWE-638: Not Using Complete Mediation *(p.1413)*
- CWE-989: SFP Secondary Cluster: Unrestricted Lock *(p.2434)*
  - CWE-412: Unrestricted Externally Accessible Lock *(p.1007)*

- CWE-895: SFP Primary Cluster: Information Leak *(p.2405)*
  - CWE-963: SFP Secondary Cluster: Exposed Data *(p.2421)*
    - CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
    - CWE-117: Improper Output Neutralization for Logs *(p.294)*
    - CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page *(p.11)*
    - CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
    - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
    - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.511)*
    - CWE-201: Insertion of Sensitive Information Into Sent Data *(p.521)*
    - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
    - CWE-210: Self-generated Error Message Containing Sensitive Information *(p.546)*
    - CWE-211: Externally-Generated Error Message Containing Sensitive Information *(p.548)*
    - CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.551)*
    - CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.555)*
    - CWE-214: Invocation of Process Using Visible Sensitive Information *(p.556)*
    - CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.558)*
    - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.560)*
    - CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.562)*
    - CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.569)*
    - CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.598)*
    - CWE-256: Plaintext Storage of a Password *(p.622)*
    - CWE-257: Storing Passwords in a Recoverable Format *(p.625)*
    - CWE-260: Password in Configuration File *(p.636)*
    - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
    - CWE-312: Cleartext Storage of Sensitive Information *(p.771)*
    - CWE-313: Cleartext Storage in a File or on Disk *(p.777)*
    - CWE-314: Cleartext Storage in the Registry *(p.779)*
    - CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.781)*
    - CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.782)*
    - CWE-317: Cleartext Storage of Sensitive Information in GUI *(p.784)*
    - CWE-318: Cleartext Storage of Sensitive Information in Executable *(p.785)*
    - CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
    - CWE-374: Passing Mutable Objects to an Untrusted Method *(p.927)*
    - CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.930)*
    - CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') *(p.984)*
    - CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.985)*
    - CWE-433: Unparsed Raw Web Content Delivery *(p.1053)*

- CWE-495: Private Data Structure Returned From A Public Method *(p.1197)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1201)*
- CWE-498: Cloneable Class Containing Sensitive Information *(p.1204)*
- CWE-499: Serializable Class Containing Sensitive Data *(p.1206)*
- CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
- CWE-501: Trust Boundary Violation *(p.1210)*
- CWE-522: Insufficiently Protected Credentials *(p.1234)*
- CWE-523: Unprotected Transport of Credentials *(p.1239)*
- CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1243)*
- CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1245)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1246)*
- CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1247)*
- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1248)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1250)*
- CWE-535: Exposure of Information Through Shell Error Message *(p.1253)*
- CWE-536: Servlet Runtime Error Message Containing Sensitive Information *(p.1254)*
- CWE-537: Java Runtime Error Message Containing Sensitive Information *(p.1255)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1257)*
- CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1259)*
- CWE-540: Inclusion of Sensitive Information in Source Code *(p.1260)*
- CWE-541: Inclusion of Sensitive Information in an Include File *(p.1262)*
- CWE-546: Suspicious Comment *(p.1266)*
- CWE-548: Exposure of Information Through Directory Listing *(p.1269)*
- CWE-550: Server-generated Error Message Containing Sensitive Information *(p.1272)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1274)*
- CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1279)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1338)*
- CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1349)*
- CWE-607: Public Static Final Field References Mutable Object *(p.1368)*
- CWE-612: Improper Authorization of Index Containing Sensitive Information *(p.1379)*
- CWE-615: Inclusion of Sensitive Information in Source Code Comments *(p.1383)*
- CWE-642: External Control of Critical State Data *(p.1422)*
- CWE-668: Exposure of Resource to Wrong Sphere *(p.1478)*
- CWE-669: Incorrect Resource Transfer Between Spheres *(p.1480)*
- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*
- CWE-756: Missing Custom Error Page *(p.1588)*
- CWE-767: Access to Critical Private Variable via Public Method *(p.1619)*
- CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote *(p.6)*

CWE-964: SFP Secondary Cluster: Exposure Temporary File *(p.2423)*
- CWE-377: Insecure Temporary File *(p.932)*
- CWE-378: Creation of Temporary File With Insecure Permissions *(p.935)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.937)*

CWE-965: SFP Secondary Cluster: Insecure Session Management *(p.2424)*
- CWE-488: Exposure of Data Element to Wrong Session *(p.1176)*
- CWE-524: Use of Cache Containing Sensitive Information *(p.1240)*
- CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length *(p.2)*

CWE-966: SFP Secondary Cluster: Other Exposures *(p.2424)*
- CWE-453: Insecure Default Variable Initialization *(p.1091)*
- CWE-487: Reliance on Package-level Scope *(p.1175)*
- CWE-492: Use of Inner Class Containing Sensitive Data *(p.1183)*
- CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1242)*
- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute *(p.1382)*
- CWE-651: Exposure of WSDL File Containing Sensitive Information *(p.1442)*

CWE-967: SFP Secondary Cluster: State Disclosure *(p.2424)*

- CWE-202: Exposure of Sensitive Information Through Data Queries *(p.523)*
- CWE-203: Observable Discrepancy *(p.525)*
- CWE-204: Observable Response Discrepancy *(p.530)*
- CWE-205: Observable Behavioral Discrepancy *(p.533)*
- CWE-206: Observable Internal Behavioral Discrepancy *(p.534)*
- CWE-207: Observable Behavioral Discrepancy With Equivalent Products *(p.535)*
- CWE-208: Observable Timing Discrepancy *(p.537)*

CWE-896: SFP Primary Cluster: Tainted Input *(p.2406)*

- CWE-990: SFP Secondary Cluster: Tainted Input to Command *(p.2434)*
  - CWE-102: Struts: Duplicate Validation Forms *(p.252)*
  - CWE-103: Struts: Incomplete validate() Method Definition *(p.254)*
  - CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.257)*
  - CWE-105: Struts: Form Field Without Validator *(p.259)*
  - CWE-106: Struts: Plug-in Framework not in Use *(p.262)*
  - CWE-107: Struts: Unused Validation Form *(p.265)*
  - CWE-108: Struts: Unvalidated Action Form *(p.267)*
  - CWE-109: Struts: Validator Turned Off *(p.269)*
  - CWE-110: Struts: Validator Without Form Field *(p.270)*
  - CWE-112: Missing XML Validation *(p.275)*
  - CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.277)*
  - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.357)*
  - CWE-134: Use of Externally-Controlled Format String *(p.371)*
  - CWE-138: Improper Neutralization of Special Elements *(p.379)*
  - CWE-140: Improper Neutralization of Delimiters *(p.382)*
  - CWE-141: Improper Neutralization of Parameter/Argument Delimiters *(p.384)*
  - CWE-142: Improper Neutralization of Value Delimiters *(p.386)*
  - CWE-143: Improper Neutralization of Record Delimiters *(p.387)*
  - CWE-144: Improper Neutralization of Line Delimiters *(p.389)*
  - CWE-145: Improper Neutralization of Section Delimiters *(p.391)*
  - CWE-146: Improper Neutralization of Expression/Command Delimiters *(p.393)*
  - CWE-147: Improper Neutralization of Input Terminators *(p.395)*
  - CWE-148: Improper Neutralization of Input Leaders *(p.397)*
  - CWE-149: Improper Neutralization of Quoting Syntax *(p.398)*
  - CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences *(p.400)*
  - CWE-151: Improper Neutralization of Comment Delimiters *(p.402)*
  - CWE-152: Improper Neutralization of Macro Symbols *(p.404)*
  - CWE-153: Improper Neutralization of Substitution Characters *(p.406)*
  - CWE-154: Improper Neutralization of Variable Name Delimiters *(p.407)*
  - CWE-155: Improper Neutralization of Wildcards or Matching Symbols *(p.409)*
  - CWE-156: Improper Neutralization of Whitespace *(p.411)*
  - CWE-157: Failure to Sanitize Paired Delimiters *(p.413)*
  - CWE-158: Improper Neutralization of Null Byte or NUL Character *(p.415)*
  - CWE-159: Improper Handling of Invalid Use of Special Elements *(p.417)*
  - CWE-160: Improper Neutralization of Leading Special Elements *(p.419)*
  - CWE-161: Improper Neutralization of Multiple Leading Special Elements *(p.421)*
  - CWE-162: Improper Neutralization of Trailing Special Elements *(p.423)*
  - CWE-163: Improper Neutralization of Multiple Trailing Special Elements *(p.425)*
  - CWE-164: Improper Neutralization of Internal Special Elements *(p.426)*
  - CWE-165: Improper Neutralization of Multiple Internal Special Elements *(p.428)*
  - CWE-183: Permissive List of Allowed Inputs *(p.464)*
  - CWE-184: Incomplete List of Disallowed Inputs *(p.466)*
  - CWE-185: Incorrect Regular Expression *(p.469)*
  - CWE-186: Overly Restrictive Regular Expression *(p.472)*

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1075)*
- CWE-553: Command Shell in Externally Accessible Directory *(p.1277)*
- CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework *(p.1278)*
- CWE-564: SQL Injection: Hibernate *(p.1290)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1376)*
- CWE-619: Dangling Database Cursor ('Cursor Injection') *(p.1391)*
- CWE-621: Variable Extraction Error *(p.1394)*
- CWE-624: Executable Regular Expression Error *(p.1399)*
- CWE-625: Permissive Regular Expression *(p.1400)*
- CWE-626: Null Byte Interaction Error (Poison Null Byte) *(p.1403)*
- CWE-627: Dynamic Variable Evaluation *(p.1405)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1421)*
- CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1428)*
- CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(p.1430)*
- CWE-646: Reliance on File Name or Extension of Externally-Supplied File *(p.1434)*
- CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1444)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1518)*
- CWE-707: Improper Neutralization *(p.1554)*
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.138)*
- CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) *(p.145)*
- CWE-76: Improper Neutralization of Equivalent Special Elements *(p.146)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.148)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) *(p.182)*
- CWE-81: Improper Neutralization of Script in an Error Message Web Page *(p.184)*
- CWE-82: Improper Neutralization of Script in Attributes of IMG Tags in a Web Page *(p.186)*
- CWE-83: Improper Neutralization of Script in Attributes in a Web Page *(p.188)*
- CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page *(p.190)*
- CWE-85: Doubled Character XSS Manipulations *(p.192)*
- CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages *(p.194)*
- CWE-87: Improper Neutralization of Alternate XSS Syntax *(p.196)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.217)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.220)*
- CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.222)*
- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.232)*
- CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.238)*
- CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.241)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.249)*

CWE-991: SFP Secondary Cluster: Tainted Input to Environment *(p.2437)*

- CWE-114: Process Control *(p.283)*

- CWE-427: Uncontrolled Search Path Element *(p.1040)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1125)*
- CWE-471: Modification of Assumed-Immutable Data (MAID) *(p.1129)*
- CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1131)*
- CWE-473: PHP External Variable Modification *(p.1134)*
- CWE-494: Download of Code Without Integrity Check *(p.1192)*
- CWE-622: Improper Validation of Function Hook Arguments *(p.1396)*
- CWE-673: External Influence of Sphere Definition *(p.1492)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.225)*

CWE-992: SFP Secondary Cluster: Faulty Input Transformation *(p.2437)*

- CWE-116: Improper Encoding or Escaping of Output *(p.287)*
- CWE-166: Improper Handling of Missing Special Element *(p.429)*
- CWE-167: Improper Handling of Additional Special Element *(p.431)*
- CWE-168: Improper Handling of Inconsistent Special Elements *(p.433)*
- CWE-172: Encoding Error *(p.439)*
- CWE-173: Improper Handling of Alternate Encoding *(p.441)*
- CWE-174: Double Decoding of the Same Data *(p.443)*
- CWE-175: Improper Handling of Mixed Encoding *(p.445)*
- CWE-176: Improper Handling of Unicode Encoding *(p.446)*
- CWE-177: Improper Handling of URL Encoding (Hex Encoding) *(p.449)*
- CWE-178: Improper Handling of Case Sensitivity *(p.451)*
- CWE-179: Incorrect Behavior Order: Early Validation *(p.454)*
- CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.457)*
- CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.460)*
- CWE-182: Collapse of Data into Unsafe Value *(p.462)*

CWE-993: SFP Secondary Cluster: Incorrect Input Handling *(p.2438)*

- CWE-198: Use of Incorrect Byte Ordering *(p.510)*
- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.575)*
- CWE-229: Improper Handling of Values *(p.577)*
- CWE-230: Improper Handling of Missing Values *(p.578)*
- CWE-231: Improper Handling of Extra Values *(p.579)*
- CWE-232: Improper Handling of Undefined Values *(p.580)*
- CWE-233: Improper Handling of Parameters *(p.581)*
- CWE-234: Failure to Handle Missing Parameter *(p.583)*
- CWE-235: Improper Handling of Extra Parameters *(p.585)*
- CWE-236: Improper Handling of Undefined Parameters *(p.586)*
- CWE-237: Improper Handling of Structural Elements *(p.587)*
- CWE-238: Improper Handling of Incomplete Structural Elements *(p.588)*
- CWE-239: Failure to Handle Incomplete Element *(p.589)*
- CWE-240: Improper Handling of Inconsistent Structural Elements *(p.590)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.591)*
- CWE-351: Insufficient Type Distinction *(p.873)*
- CWE-354: Improper Validation of Integrity Check Value *(p.883)*

CWE-994: SFP Secondary Cluster: Tainted Input to Variable *(p.2438)*

- CWE-15: External Control of System or Configuration Setting *(p.17)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1092)*
- CWE-496: Public Data Assigned to Private Array-Typed Field *(p.1199)*
- CWE-502: Deserialization of Untrusted Data *(p.1212)*
- CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1294)*
- CWE-606: Unchecked Input for Loop Condition *(p.1366)*
- CWE-616: Incomplete Identification of Uploaded File Variables (PHP) *(p.1385)*

CWE-897: SFP Primary Cluster: Entry Points *(p.2406)*

- CWE-1002: SFP Secondary Cluster: Unexpected Entry Points *(p.2442)*
  - CWE-489: Active Debug Code *(p.1178)*
  - CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1181)*
  - CWE-493: Critical Public Variable Without Final Modifier *(p.1190)*
  - CWE-500: Public Static Field Not Marked Final *(p.1208)*
  - CWE-531: Inclusion of Sensitive Information in Test Code *(p.1249)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1299)*
  - CWE-580: clone() Method Without super.clone() *(p.1319)*
  - CWE-582: Array Declared Public, Final, and Static *(p.1322)*
  - CWE-583: finalize() Method Declared Public *(p.1324)*
  - CWE-608: Struts: Non-private Field in ActionForm Class *(p.1369)*
  - CWE-766: Critical Data Element Declared Public *(p.1615)*
- CWE-898: SFP Primary Cluster: Authentication *(p.2406)*
  - CWE-947: SFP Secondary Cluster: Authentication Bypass *(p.2415)*
    - CWE-287: Improper Authentication *(p.699)*
    - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.707)*
    - CWE-289: Authentication Bypass by Alternate Name *(p.710)*
    - CWE-303: Incorrect Implementation of Authentication Algorithm *(p.744)*
    - CWE-304: Missing Critical Step in Authentication *(p.745)*
    - CWE-305: Authentication Bypass by Primary Weakness *(p.747)*
    - CWE-308: Use of Single-factor Authentication *(p.759)*
    - CWE-309: Use of Password System for Primary Authentication *(p.761)*
    - CWE-603: Use of Client-Side Authentication *(p.1363)*
  - CWE-948: SFP Secondary Cluster: Digital Certificate *(p.2416)*
    - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.726)*
    - CWE-297: Improper Validation of Certificate with Host Mismatch *(p.729)*
    - CWE-298: Improper Validation of Certificate Expiration *(p.733)*
    - CWE-299: Improper Check for Certificate Revocation *(p.734)*
    - CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created *(p.1339)*
    - CWE-599: Missing Validation of OpenSSL Certificate *(p.1350)*
  - CWE-949: SFP Secondary Cluster: Faulty Endpoint Authentication *(p.2416)*
    - CWE-293: Using Referer Field for Authentication *(p.717)*
    - CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.742)*
    - CWE-345: Insufficient Verification of Data Authenticity *(p.858)*
    - CWE-346: Origin Validation Error *(p.860)*
    - CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action *(p.870)*
    - CWE-360: Trust of System Event Data *(p.894)*
    - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1273)*
    - CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1292)*
    - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1435)*
  - CWE-950: SFP Secondary Cluster: Hardcoded Sensitive Data *(p.2417)*
    - CWE-258: Empty Password in Configuration File *(p.628)*
    - CWE-259: Use of Hard-coded Password *(p.630)*
    - CWE-321: Use of Hard-coded Cryptographic Key *(p.792)*
    - CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1267)*
  - CWE-951: SFP Secondary Cluster: Insecure Authentication Policy *(p.2417)*
    - CWE-262: Not Using Password Aging *(p.640)*
    - CWE-263: Password Aging with Long Expiration *(p.643)*
    - CWE-521: Weak Password Requirements *(p.1231)*
    - CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1280)*
    - CWE-613: Insufficient Session Expiration *(p.1380)*
    - CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1432)*
  - CWE-952: SFP Secondary Cluster: Missing Authentication *(p.2417)*
    - CWE-306: Missing Authentication for Critical Function *(p.748)*

- CWE-620: Unverified Password Change *(p.1392)*
- CWE-953: SFP Secondary Cluster: Missing Endpoint Authentication *(p.2418)*
  - CWE-422: Unprotected Windows Messaging Channel ('Shatter') *(p.1029)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
- CWE-954: SFP Secondary Cluster: Multiple Binds to the Same Port *(p.2418)*
  - CWE-605: Multiple Binds to the Same Port *(p.1364)*
- CWE-955: SFP Secondary Cluster: Unrestricted Authentication *(p.2418)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.754)*

CWE-899: SFP Primary Cluster: Access Control *(p.2407)*

- CWE-944: SFP Secondary Cluster: Access Management *(p.2414)*
  - CWE-282: Improper Ownership Management *(p.683)*
  - CWE-283: Unverified Ownership *(p.685)*
  - CWE-284: Improper Access Control *(p.687)*
  - CWE-286: Incorrect User Management *(p.698)*
  - CWE-708: Incorrect Ownership Assignment *(p.1556)*
- CWE-945: SFP Secondary Cluster: Insecure Resource Access *(p.2415)*
  - CWE-285: Improper Authorization *(p.691)*
  - CWE-424: Improper Protection of Alternate Path *(p.1031)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
  - CWE-650: Trusting HTTP Permission Methods on the Server Side *(p.1441)*
- CWE-946: SFP Secondary Cluster: Insecure Resource Permissions *(p.2415)*
  - CWE-276: Incorrect Default Permissions *(p.672)*
  - CWE-277: Insecure Inherited Permissions *(p.675)*
  - CWE-278: Insecure Preserved Inherited Permissions *(p.676)*
  - CWE-279: Incorrect Execution-Assigned Permissions *(p.678)*
  - CWE-281: Improper Preservation of Permissions *(p.681)*
  - CWE-560: Use of umask() with chmod-style Argument *(p.1282)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*

CWE-901: SFP Primary Cluster: Privilege *(p.2407)*

- CWE-250: Execution with Unnecessary Privileges *(p.606)*
- CWE-266: Incorrect Privilege Assignment *(p.645)*
- CWE-267: Privilege Defined With Unsafe Actions *(p.648)*
- CWE-268: Privilege Chaining *(p.651)*
- CWE-269: Improper Privilege Management *(p.653)*
- CWE-270: Privilege Context Switching Error *(p.659)*
- CWE-271: Privilege Dropping / Lowering Errors *(p.660)*
- CWE-272: Least Privilege Violation *(p.663)*
- CWE-274: Improper Handling of Insufficient Privileges *(p.670)*
- CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1230)*
- CWE-653: Improper Isolation or Compartmentalization *(p.1445)*
- CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*

CWE-902: SFP Primary Cluster: Channel *(p.2408)*

- CWE-956: SFP Secondary Cluster: Channel Attack *(p.2418)*
  - CWE-290: Authentication Bypass by Spoofing *(p.712)*
  - CWE-294: Authentication Bypass by Capture-replay *(p.719)*
  - CWE-300: Channel Accessible by Non-Endpoint *(p.737)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.740)*
  - CWE-419: Unprotected Primary Channel *(p.1024)*
  - CWE-420: Unprotected Alternate Channel *(p.1025)*
  - CWE-421: Race Condition During Access to Alternate Channel *(p.1028)*
  - CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1072)*
- CWE-957: SFP Secondary Cluster: Protocol Error *(p.2419)*
  - CWE-353: Missing Support for Integrity Check *(p.881)*
  - CWE-435: Improper Interaction Between Multiple Correctly-Behaving Entities *(p.1063)*
  - CWE-436: Interpretation Conflict *(p.1065)*

- CWE-437: Incomplete Model of Endpoint Features *(p.1067)*
- CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') *(p.1589)*

CWE-903: SFP Primary Cluster: Cryptography *(p.2408)*
- CWE-958: SFP Secondary Cluster: Broken Cryptography *(p.2419)*
  - CWE-325: Missing Cryptographic Step *(p.801)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-328: Use of Weak Hash *(p.813)*
  - CWE-759: Use of a One-Way Hash without a Salt *(p.1593)*
  - CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1598)*
- CWE-959: SFP Secondary Cluster: Weak Cryptography *(p.2419)*
  - CWE-261: Weak Encoding for Password *(p.638)*
  - CWE-322: Key Exchange without Entity Authentication *(p.795)*
  - CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.797)*
  - CWE-324: Use of a Key Past its Expiration Date *(p.799)*
  - CWE-326: Inadequate Encryption Strength *(p.803)*
  - CWE-329: Generation of Predictable IV with CBC Mode *(p.818)*
  - CWE-347: Improper Verification of Cryptographic Signature *(p.864)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1418)*

CWE-904: SFP Primary Cluster: Malware *(p.2408)*
- CWE-506: Embedded Malicious Code *(p.1218)*
- CWE-507: Trojan Horse *(p.1220)*
- CWE-508: Non-Replicating Malicious Code *(p.1221)*
- CWE-509: Replicating Malicious Code (Virus or Worm) *(p.1222)*
- CWE-510: Trapdoor *(p.1223)*
- CWE-511: Logic/Time Bomb *(p.1225)*
- CWE-512: Spyware *(p.1226)*
- CWE-69: Improper Handling of Windows ::DATA Alternate Data Stream *(p.130)*
- CWE-968: SFP Secondary Cluster: Covert Channel *(p.2425)*
  - CWE-385: Covert Timing Channel *(p.947)*
  - CWE-514: Covert Channel *(p.1227)*
  - CWE-515: Covert Storage Channel *(p.1229)*

CWE-905: SFP Primary Cluster: Predictability *(p.2409)*
- CWE-330: Use of Insufficiently Random Values *(p.821)*
- CWE-331: Insufficient Entropy *(p.828)*
- CWE-332: Insufficient Entropy in PRNG *(p.830)*
- CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.832)*
- CWE-334: Small Space of Random Values *(p.834)*
- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.836)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.839)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.841)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.844)*
- CWE-339: Small Seed Space in PRNG *(p.847)*
- CWE-340: Generation of Predictable Numbers or Identifiers *(p.849)*
- CWE-341: Predictable from Observable State *(p.850)*
- CWE-342: Predictable Exact Value from Previous Values *(p.852)*
- CWE-343: Predictable Value Range from Previous Values *(p.854)*
- CWE-344: Use of Invariant Value in Dynamically Changing Context *(p.856)*

CWE-906: SFP Primary Cluster: UI *(p.2409)*
- CWE-995: SFP Secondary Cluster: Feature *(p.2439)*
  - CWE-447: Unimplemented or Unsupported Feature in UI *(p.1082)*
  - CWE-448: Obsolete Feature in UI *(p.1083)*
  - CWE-449: The UI Performs the Wrong Action *(p.1084)*
  - CWE-450: Multiple Interpretations of UI Input *(p.1085)*
  - CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1087)*

- CWE-549: Missing Password Field Masking *(p.1271)*
- CWE-655: Insufficient Psychological Acceptability *(p.1450)*

- CWE-996: SFP Secondary Cluster: Security *(p.2439)*
  - CWE-356: Product UI does not Warn User of Unsafe Actions *(p.886)*
  - CWE-357: Insufficient UI Warning of Dangerous Operations *(p.887)*
  - CWE-446: UI Discrepancy for Security Feature *(p.1081)*
- CWE-997: SFP Secondary Cluster: Information Loss *(p.2439)*
  - CWE-221: Information Loss or Omission *(p.563)*
  - CWE-222: Truncation of Security-relevant Information *(p.565)*
  - CWE-223: Omission of Security-relevant Information *(p.566)*
  - CWE-224: Obscured Security-relevant Information by Alternate Name *(p.568)*

- CWE-907: SFP Primary Cluster: Other *(p.2409)*
  - CWE-975: SFP Secondary Cluster: Architecture *(p.2427)*
    - CWE-348: Use of Less Trusted Source *(p.866)*
    - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.889)*
    - CWE-602: Client-Side Enforcement of Server-Side Security *(p.1359)*
    - CWE-637: Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism') *(p.1411)*
    - CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1439)*
    - CWE-654: Reliance on a Single Factor in a Security Decision *(p.1448)*
    - CWE-656: Reliance on Security Through Obscurity *(p.1452)*
    - CWE-657: Violation of Secure Design Principles *(p.1454)*
    - CWE-671: Lack of Administrator Control over Security *(p.1487)*
    - CWE-693: Protection Mechanism Failure *(p.1529)*
    - CWE-749: Exposed Dangerous Method or Function *(p.1572)*
  - CWE-976: SFP Secondary Cluster: Compiler *(p.2428)*
    - CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1570)*
  - CWE-977: SFP Secondary Cluster: Design *(p.2428)*
    - CWE-115: Misinterpretation of Input *(p.286)*
    - CWE-187: Partial String Comparison *(p.474)*
    - CWE-188: Reliance on Data/Memory Layout *(p.476)*
    - CWE-193: Off-by-one Error *(p.493)*
    - CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.868)*
    - CWE-405: Asymmetric Resource Consumption (Amplification) *(p.993)*
    - CWE-406: Insufficient Control of Network Message Volume (Network Amplification) *(p.997)*
    - CWE-407: Inefficient Algorithmic Complexity *(p.999)*
    - CWE-408: Incorrect Behavior Order: Early Amplification *(p.1002)*
    - CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.1004)*
    - CWE-410: Insufficient Resource Pool *(p.1005)*
    - CWE-430: Deployment of Wrong Handler *(p.1049)*
    - CWE-462: Duplicate Key in Associative List (Alist) *(p.1111)*
    - CWE-463: Deletion of Data Structure Sentinel *(p.1113)*
    - CWE-464: Addition of Data Structure Sentinel *(p.1115)*
    - CWE-483: Incorrect Block Delimitation *(p.1167)*
    - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1321)*
    - CWE-595: Comparison of Object References Instead of Object Contents *(p.1342)*
    - CWE-618: Exposed Unsafe ActiveX Method *(p.1389)*
    - CWE-648: Incorrect Use of Privileged APIs *(p.1437)*
    - CWE-670: Always-Incorrect Control Flow Implementation *(p.1484)*
    - CWE-682: Incorrect Calculation *(p.1507)*
    - CWE-691: Insufficient Control Flow Management *(p.1525)*
    - CWE-696: Incorrect Behavior Order *(p.1535)*
    - CWE-697: Incorrect Comparison *(p.1538)*
    - CWE-698: Execution After Redirect (EAR) *(p.1542)*

- CWE-705: Incorrect Control Flow Scoping *(p.1550)*
- CWE-978: SFP Secondary Cluster: Implementation *(p.2429)*
  - CWE-358: Improperly Implemented Security Check for Standard *(p.888)*
  - CWE-398: 7PK - Code Quality *(p.2344)*
  - CWE-623: Unsafe ActiveX Control Marked Safe For Scripting *(p.1397)*
  - CWE-710: Improper Adherence to Coding Standards *(p.1558)*
- CWE-1237: SFP Primary Cluster: Faulty Resource Release *(p.2503)*
  - CWE-415: Double Free *(p.1015)*
  - CWE-762: Mismatched Memory Management Routines *(p.1605)*
  - CWE-763: Release of Invalid Pointer or Reference *(p.1608)*
- CWE-1238: SFP Primary Cluster: Failure to Release Memory *(p.2503)*
  - CWE-401: Missing Release of Memory after Effective Lifetime *(p.980)*

Graph View: CWE-900: Weaknesses in the 2011 CWE/ SANS Top 25 Most Dangerous Software Errors

- CWE-867: 2011 Top 25 - Weaknesses On the Cusp *(p.2393)*
  - CWE-129: Improper Validation of Array Index *(p.347)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.551)*
  - CWE-330: Use of Insufficiently Random Values *(p.821)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.895)*
  - CWE-456: Missing Initialization of a Variable *(p.1096)*
  - CWE-476: NULL Pointer Dereference *(p.1139)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1504)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1577)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1622)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1632)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1711)*
  - CWE-822: Untrusted Pointer Dereference *(p.1732)*
  - CWE-825: Expired Pointer Dereference *(p.1741)*
  - CWE-838: Inappropriate Encoding for Output Context *(p.1773)*
  - CWE-841: Improper Enforcement of Behavioral Workflow *(p.1781)*
- CWE-866: 2011 Top 25 - Porous Defenses *(p.2393)*
  - CWE-250: Execution with Unnecessary Privileges *(p.606)*
  - CWE-306: Missing Authentication for Critical Function *(p.748)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.754)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
  - CWE-759: Use of a One-Way Hash without a Salt *(p.1593)*
  - CWE-798: Use of Hard-coded Credentials *(p.1699)*
  - CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1723)*
  - CWE-862: Missing Authorization *(p.1789)*
  - CWE-863: Incorrect Authorization *(p.1796)*
- CWE-865: 2011 Top 25 - Risky Resource Management *(p.2392)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.310)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.361)*
  - CWE-134: Use of Externally-Controlled Format String *(p.371)*
  - CWE-190: Integer Overflow or Wraparound *(p.478)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-494: Download of Code Without Integrity Check *(p.1192)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1498)*
- CWE-864: 2011 Top 25 - Insecure Interaction Between Components *(p.2392)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.875)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1055)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
  - CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1750)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*

Graph View: CWE-928: Weaknesses in OWASP Top Ten (2013)

- CWE-929: OWASP Top Ten 2013 Category A1 - Injection *(p.2410)*
  - CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.138)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.148)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.155)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.198)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.206)*
    - CWE-564: SQL Injection: Hibernate *(p.1290)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.217)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.220)*
  - CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1428)*
  - CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1444)*
- CWE-930: OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management *(p.2410)*
  - CWE-256: Plaintext Storage of a Password *(p.622)*
  - CWE-287: Improper Authentication *(p.699)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-384: Session Fixation *(p.943)*
  - CWE-522: Insufficiently Protected Credentials *(p.1234)*
  - CWE-523: Unprotected Transport of Credentials *(p.1239)*
  - CWE-613: Insufficient Session Expiration *(p.1380)*
  - CWE-620: Unverified Password Change *(p.1392)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1418)*
- CWE-931: OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS) *(p.2411)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.168)*
- CWE-932: OWASP Top Ten 2013 Category A4 - Insecure Direct Object References *(p.2411)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.249)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
  - CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1553)*
- CWE-933: OWASP Top Ten 2013 Category A5 - Security Misconfiguration *(p.2412)*
  - CWE-2: 7PK - Environment *(p.2329)*
  - CWE-16: Configuration *(p.2330)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.540)*
  - CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.558)*
  - CWE-548: Exposure of Information Through Directory Listing *(p.1269)*
- CWE-934: OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure *(p.2412)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.764)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.771)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.786)*
  - CWE-320: Key Management Errors *(p.2340)*
  - CWE-325: Missing Cryptographic Step *(p.801)*
  - CWE-326: Inadequate Encryption Strength *(p.803)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.806)*
  - CWE-328: Use of Weak Hash *(p.813)*
- CWE-935: OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control *(p.2413)*
  - CWE-285: Improper Authorization *(p.691)*
- CWE-936: OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF) *(p.2413)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.875)*
- CWE-937: OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities *(p.2413)*

- CWE-938: OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards *(p.2414)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1353)*

Graph View: CWE-1000: Research Concepts

- CWE-284: Improper Access Control *(p.687)*
  - CWE-1191: On-Chip Debug and Test Interface With Improper Access Control *(p.1989)*
  - CWE-1220: Insufficient Granularity of Access Control *(p.2002)*
    - CWE-1222: Insufficient Granularity of Address Regions Protected by Register Locks *(p.2010)*
  - CWE-1224: Improper Restriction of Write-Once Bit Fields *(p.2014)*
  - CWE-1231: Improper Prevention of Lock Bit Modification *(p.2018)*
  - CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2023)*
  - CWE-1242: Inclusion of Undocumented Features or Chicken Bits *(p.2044)*
  - CWE-1252: CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations *(p.2068)*
  - CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions *(p.2079)*
  - CWE-1259: Improper Restriction of Security Token Assignment *(p.2085)*
  - CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges *(p.2087)*
  - CWE-1262: Improper Access Control for Register Interface *(p.2093)*
  - CWE-1263: Improper Physical Access Control *(p.2097)*
    - CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug *(p.2046)*
  - CWE-1267: Policy Uses Obsolete Encoding *(p.2105)*
  - CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents *(p.2107)*
  - CWE-1270: Generation of Incorrect Security Tokens *(p.2113)*
  - CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code *(p.2121)*
  - CWE-1276: Hardware Child Block Incorrectly Connected to Parent System *(p.2125)*
  - CWE-1280: Access Control Check Implemented After Asset is Accessed *(p.2134)*
  - CWE-1283: Mutable Attestation or Measurement Reporting Data *(p.2140)*
  - CWE-1290: Incorrect Decoding of Security Identifiers *(p.2155)*
  - CWE-1292: Incorrect Conversion of Security Identifiers *(p.2159)*
  - CWE-1294: Insecure Security Identifier Mechanism *(p.2162)*
    - CWE-1302: Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC) *(p.2185)*
  - CWE-1296: Incorrect Chaining or Granularity of Debug Components *(p.2166)*
  - CWE-1304: Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation *(p.2188)*
  - CWE-1311: Improper Translation of Security Attributes by Fabric Bridge *(p.2194)*
  - CWE-1312: Missing Protection for Mirrored Regions in On-Chip Fabric Firewall *(p.2196)*
  - CWE-1313: Hardware Allows Activation of Test or Debug Logic at Runtime *(p.2198)*
  - CWE-1315: Improper Setting of Bus Controlling Capability in Fabric End-point *(p.2202)*
  - CWE-1316: Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges *(p.2204)*
  - CWE-1317: Improper Access Control in Fabric Bridge *(p.2206)*
  - CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals *(p.2214)*
  - CWE-1323: Improper Management of Sensitive Trace Data *(p.2220)*
  - CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy *(p.2246)*
  - CWE-269: Improper Privilege Management *(p.653)*
    - CWE-250: Execution with Unnecessary Privileges *(p.606)*
    - CWE-266: Incorrect Privilege Assignment *(p.645)*
      - CWE-1022: Use of Web Link to Untrusted Target with window.opener Access *(p.1872)*
      - CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1230)*
      - CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1280)*
      - CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*
    - CWE-267: Privilege Defined With Unsafe Actions *(p.648)*
      - CWE-623: Unsafe ActiveX Control Marked Safe For Scripting *(p.1397)*
    - CWE-268: Privilege Chaining *(p.651)*
    - CWE-270: Privilege Context Switching Error *(p.659)*
    - CWE-271: Privilege Dropping / Lowering Errors *(p.660)*
      - CWE-272: Least Privilege Violation *(p.663)*

- CWE-273: Improper Check for Dropped Privileges *(p.667)*
- CWE-274: Improper Handling of Insufficient Privileges *(p.670)*
- CWE-648: Incorrect Use of Privileged APIs *(p.1437)*

CWE-282: Improper Ownership Management *(p.683)*
- CWE-283: Unverified Ownership *(p.685)*
- CWE-708: Incorrect Ownership Assignment *(p.1556)*

CWE-285: Improper Authorization *(p.691)*
- CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2017)*
  - CWE-202: Exposure of Sensitive Information Through Data Queries *(p.523)*
  - CWE-612: Improper Authorization of Index Containing Sensitive Information *(p.1379)*
- CWE-1256: Improper Restriction of Software Interfaces to Hardware Features *(p.2076)*
- CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT Vendors *(p.2168)*
- CWE-1328: Security Version Number Mutable to Older Versions *(p.2229)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1274)*
  - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.560)*
    - CWE-433: Unparsed Raw Web Content Delivery *(p.1053)*
  - CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.562)*
  - CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1245)*
  - CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1246)*
  - CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1247)*
  - CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1248)*
  - CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1259)*
  - CWE-553: Command Shell in Externally Accessible Directory *(p.1277)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1559)*
  - CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag *(p.1863)*
  - CWE-276: Incorrect Default Permissions *(p.672)*
  - CWE-277: Insecure Inherited Permissions *(p.675)*
  - CWE-278: Insecure Preserved Inherited Permissions *(p.676)*
  - CWE-279: Incorrect Execution-Assigned Permissions *(p.678)*
  - CWE-281: Improper Preservation of Permissions *(p.681)*
  - CWE-766: Critical Data Element Declared Public *(p.1615)*
- CWE-862: Missing Authorization *(p.1789)*
  - CWE-1314: Missing Write Protection for Parametric Data Values *(p.2199)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
  - CWE-638: Not Using Complete Mediation *(p.1413)*
    - CWE-424: Improper Protection of Alternate Path *(p.1031)*
      - CWE-425: Direct Request ('Forced Browsing') *(p.1032)*
  - CWE-939: Improper Authorization in Handler for Custom URL Scheme *(p.1849)*
- CWE-863: Incorrect Authorization *(p.1796)*
  - CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State *(p.2048)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1273)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1415)*
    - CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1294)*
  - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1435)*
  - CWE-804: Guessable CAPTCHA *(p.1710)*
  - CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1857)*
- CWE-926: Improper Export of Android Application Components *(p.1843)*
- CWE-927: Use of Implicit Intent for Sensitive Communication *(p.1846)*

CWE-286: Incorrect User Management *(p.698)*
- CWE-842: Placement of User into Incorrect Group *(p.1784)*

CWE-287: Improper Authentication *(p.699)*
- CWE-1390: Weak Authentication *(p.2279)*