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	2593
HasMember	C	2	7PK - Environment	1344	2308
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	2309
HasMember	B	260	Password in Configuration File	1344	629
HasMember	V	315	Cleartext Storage of Sensitive Information in a Cookie	1344	774
HasMember	V	520	.NET Misconfiguration: Use of Impersonation	1344	1222
HasMember	V	526	Cleartext Storage of Sensitive Information in an Environment Variable	1344	1234
HasMember	V	537	Java Runtime Error Message Containing Sensitive Information	1344	1246
HasMember	V	541	Inclusion of Sensitive Information in an Include File	1344	1253
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	1344	1259
HasMember	B	611	Improper Restriction of XML External Entity Reference	1344	1367
HasMember	V	614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	1344	1373
HasMember	B	756	Missing Custom Error Page	1344	1579
HasMember	B	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	1344	1633
HasMember	V	942	Permissive Cross-domain Policy with Untrusted Domains	1344	1847
HasMember	V	1004	Sensitive Cookie Without 'HttpOnly' Flag	1344	1854
HasMember	C	1032	OWASP Top Ten 2017 Category A6 - Security Misconfiguration	1344	2438
HasMember	V	1174	ASP.NET Misconfiguration: Improper Model Validation	1344	1970

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	2593
HasMember	C	937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities	1344	2392
HasMember	C	1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities	1344	2439
HasMember	B	1104	Use of Unmaintained Third Party Components	1344	1944

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	2593
HasMember	C	255	Credentials Management Errors	1344	2315
HasMember	V	259	Use of Hard-coded Password	1344	623
HasMember	C	287	Improper Authentication	1344	692
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1344	700
HasMember	B	290	Authentication Bypass by Spoofing	1344	705
HasMember	B	294	Authentication Bypass by Capture-replay	1344	712
HasMember	B	295	Improper Certificate Validation	1344	714
HasMember	V	297	Improper Validation of Certificate with Host Mismatch	1344	722
HasMember	C	300	Channel Accessible by Non-Endpoint	1344	730
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	1344	735
HasMember	B	304	Missing Critical Step in Authentication	1344	738
HasMember	B	306	Missing Authentication for Critical Function	1344	741
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	1344	747
HasMember	C	346	Origin Validation Error	1344	853
HasMember		384	Session Fixation	1344	936
HasMember	B	521	Weak Password Requirements	1344	1223
HasMember	B	613	Insufficient Session Expiration	1344	1371
HasMember	B	620	Unverified Password Change	1344	1383
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	1344	1409
HasMember	B	798	Use of Hard-coded Credentials	1344	1690
HasMember	B	940	Improper Verification of Source of a Communication Channel	1344	1842
HasMember	C	1216	Lockout Mechanism Errors	1344	2478

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

Nature	Type	ID	Name	V	Page
MemberOf	V	1344	Weaknesses in OWASP Top Ten (2021)	1344	2593
HasMember	C	345	Insufficient Verification of Data Authenticity	1344	851
HasMember	B	353	Missing Support for Integrity Check	1344	874
HasMember	B	426	Untrusted Search Path	1344	1028
HasMember	B	494	Download of Code Without Integrity Check	1344	1185
HasMember	B	502	Deserialization of Untrusted Data	1344	1204
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	1344	1283
HasMember	V	784	Reliance on Cookies without Validation and Integrity Checking in a Security Decision	1344	1653
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1344	1741
HasMember	V	830	Inclusion of Web Functionality from an Untrusted Source	1344	1747
HasMember	B	915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	1344	1809

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	2593
HasMember	B	117	Improper Output Neutralization for Logs	1344	288
HasMember	B	223	Omission of Security-relevant Information	1344	559
HasMember	B	532	Insertion of Sensitive Information into Log File	1344	1241
HasMember	B	778	Insufficient Logging	1344	1638

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	2593
HasMember	B	918	Server-Side Request Forgery (SSRF)	1344	1820

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	2596
HasMember	C	1364	ICS Communications: Zone Boundary Failures	1358	2501
HasMember	C	1365	ICS Communications: Unreliability	1358	2502
HasMember	C	1366	ICS Communications: Frail Security in Protocols	1358	2503

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	2596
HasMember	C	1367	ICS Dependencies (& Architecture): External Physical Systems	1358	2504
HasMember	C	1368	ICS Dependencies (& Architecture): External Digital Systems	1358	2505

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	2596
HasMember	C	1369	ICS Supply Chain: IT/OT Convergence/Expansion	1358	2506
HasMember	C	1370	ICS Supply Chain: Common Mode Frailties	1358	2507
HasMember	C	1371	ICS Supply Chain: Poorly Documented or Undocumented Features	1358	2508
HasMember	C	1372	ICS Supply Chain: OT Counterfeit and Malicious Corruption	1358	2509

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	2596
HasMember	C	1373	ICS Engineering (Construction/Deployment): Trust Model Problems	1358	2510

Nature	Type	ID	Name	V	Page
HasMember	C	1374	ICS Engineering (Construction/Deployment): Maker Breaker Blindness	1358	2510
HasMember	C	1375	ICS Engineering (Construction/Deployment): Gaps in Details/Data	1358	2511
HasMember	C	1376	ICS Engineering (Construction/Deployment): Security Gaps in Commissioning	1358	2512
HasMember	C	1377	ICS Engineering (Construction/Deployment): Inherent Predictability in Design	1358	2513

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	2596
HasMember	C	1378	ICS Operations (& Maintenance): Gaps in obligations and training	1358	2513
HasMember	C	1379	ICS Operations (& Maintenance): Human factors in ICS environments	1358	2514
HasMember	C	1380	ICS Operations (& Maintenance): Post-analysis changes	1358	2515
HasMember	C	1381	ICS Operations (& Maintenance): Exploitable Standard Operational Procedures	1358	2516
HasMember	C	1382	ICS Operations (& Maintenance): Emerging Energy Technologies	1358	2517
HasMember	C	1383	ICS Operations (& Maintenance): Compliance/ Conformance with Regulatory Requirements	1358	2517

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	2497
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	1358	544
HasMember	B	268	Privilege Chaining	1358	644
HasMember	C	269	Improper Privilege Management	1358	646
HasMember	C	287	Improper Authentication	1358	692
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1358	700
HasMember	B	306	Missing Authentication for Critical Function	1358	741
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	888
HasMember		384	Session Fixation	1358	936
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1358	1048
HasMember	B	494	Download of Code Without Integrity Check	1358	1185
HasMember	B	501	Trust Boundary Violation	1358	1203
HasMember	C	668	Exposure of Resource to Wrong Sphere	1358	1469
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1358	1471
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1358	1568

Nature	Type	ID	Name	V	Page
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1358	1741
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1358	1976
HasMember	C	1263	Improper Physical Access Control	1358	2085
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1358	2174
HasMember	B	1393	Use of Default Password	1358	2273

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	2497
HasMember	V	121	Stack-based Buffer Overflow	1358	314
HasMember	C	269	Improper Privilege Management	1358	646
HasMember	B	306	Missing Authentication for Critical Function	1358	741
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1358	861
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	888
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1358	1714
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1358	2044
HasMember	B	1261	Improper Handling of Single Event Upsets	1358	2079

Nature	Type	ID	Name	V	Page
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1358	2227
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1358	2252
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1358	2257

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	2497
HasMember	V	121	Stack-based Buffer Overflow	1358	314
HasMember	B	125	Out-of-bounds Read	1358	330
HasMember	B	268	Privilege Chaining	1358	644
HasMember	C	269	Improper Privilege Management	1358	646
HasMember	B	276	Incorrect Default Permissions	1358	665
HasMember	B	290	Authentication Bypass by Spoofing	1358	705
HasMember	B	306	Missing Authentication for Critical Function	1358	741
HasMember	C	311	Missing Encryption of Sensitive Data	1358	757
HasMember	B	312	Cleartext Storage of Sensitive Information	1358	764

Nature	Type	ID	Name	V	Page
HasMember	B	319	Cleartext Transmission of Sensitive Information	1358	779
HasMember	B	325	Missing Cryptographic Step	1358	794
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1358	799
HasMember	C	330	Use of Insufficiently Random Values	1358	814
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1358	832
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1358	834
HasMember	B	341	Predictable from Observable State	1358	843
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1358	861
HasMember	B	358	Improperly Implemented Security Check for Standard	1358	881
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	888
HasMember	C	377	Insecure Temporary File	1358	925
HasMember	♣	384	Session Fixation	1358	936
HasMember	B	648	Incorrect Use of Privileged APIs	1358	1428
HasMember	B	787	Out-of-bounds Write	1358	1661
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1358	1976
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1358	2174
HasMember	B	1393	Use of Default Password	1358	2273

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	2498
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1358	2044
HasMember	B	1338	Improper Protections Against Hardware Overheating	1358	2240
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1358	2254
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1358	2257

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	2498
HasMember	B	15	External Control of System or Configuration Setting	1358	17
HasMember	C	287	Improper Authentication	1358	692
HasMember	B	306	Missing Authentication for Critical Function	1358	741

Nature	Type	ID	Name	V	Page
HasMember	B	308	Use of Single-factor Authentication	1358	752
HasMember	B	312	Cleartext Storage of Sensitive Information	1358	764
HasMember	B	440	Expected Behavior Violation	1358	1062
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1358	1118
HasMember	B	603	Use of Client-Side Authentication	1358	1354
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1358	1364
HasMember	C	638	Not Using Complete Mediation	1358	1404
HasMember	C	1059	Insufficient Technical Documentation	1358	1894
HasMember	B	1068	Inconsistency Between Implementation and Documented Design	1358	1906
HasMember	B	1104	Use of Unmaintained Third Party Components	1358	1944
HasMember	B	1329	Reliance on Component That is Not Updateable	1358	2219
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1358	2254
HasMember	B	1393	Use of Default Password	1358	2273

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	2499
HasMember	P	284	Improper Access Control	1358	680

Nature	Type	ID	Name	V	Page
HasMember	C	636	Not Failing Securely ('Failing Open')	1358	1401

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	2499
HasMember	V	329	Generation of Predictable IV with CBC Mode	1358	811
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1358	1454
HasMember	P	693	Protection Mechanism Failure	1358	1520
HasMember	P	707	Improper Neutralization	1358	1546
HasMember	P	710	Improper Adherence to Coding Standards	1358	1549
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	1358	2254

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	2499
HasMember	B	489	Active Debug Code	1358	1171
HasMember	C	912	Hidden Functionality	1358	1803
HasMember	C	1059	Insufficient Technical Documentation	1358	1894
HasMember	B	1242	Inclusion of Undocumented Features or Chicken Bits	1358	2033

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	2499
HasMember	P	284	Improper Access Control	1358	680
HasMember	C	1198	Privilege Separation and Access Control Issues	1358	2470
HasMember	B	1231	Improper Prevention of Lock Bit Modification	1358	2007
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	1358	2012
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1358	2118

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	2499
HasMember	C	269	Improper Privilege Management	1358	646
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1358	861
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1358	1714

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	2499

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	2499
HasMember	P	710	Improper Adherence to Coding Standards	1358	1549
HasMember	B	1053	Missing Documentation for Design	1358	1888
HasMember	C	1059	Insufficient Technical Documentation	1358	1894
HasMember	B	1110	Incomplete Design Documentation	1358	1950
HasMember	B	1111	Incomplete I/O Documentation	1358	1951

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	2499
HasMember	B	276	Incorrect Default Permissions	1358	665
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1358	888
HasMember	B	1393	Use of Default Password	1358	2273

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	2499
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1358	2118

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	2500

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 >.

[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	2500

Nature	Type	ID	Name	V	Page
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1358	1079
HasMember	C	655	Insufficient Psychological Acceptability	1358	1442

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	2500

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	2500

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	2500
HasMember	C	20	Improper Input Validation	1358	20
HasMember	C	285	Improper Authorization	1358	684
HasMember	B	295	Improper Certificate Validation	1358	714
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	1358	719
HasMember	C	346	Origin Validation Error	1358	853
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	1358	990
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1358	1345

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	2500
HasMember	P	710	Improper Adherence to Coding Standards	1358	1549

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	2586
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1194	2044
HasMember	B	1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications	1194	2049
HasMember	V	1255	Comparison Logic is Vulnerable to Power Side-Channel Attacks	1194	2062

Nature	Type	ID	Name	V	Page
HasMember	B	1261	Improper Handling of Single Event Upsets	1194	2079
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1194	2118
HasMember	B	1300	Improper Protection of Physical Side Channels	1194	2165
HasMember	B	1319	Improper Protection against Electromagnetic Fault Injection (EM-FI)	1194	2199
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1194	2227
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1194	2252
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1194	2257

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	2598
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	516
HasMember	B	256	Plaintext Storage of a Password	1400	615
HasMember	B	257	Storing Passwords in a Recoverable Format	1400	618
HasMember	V	258	Empty Password in Configuration File	1400	621
HasMember	V	259	Use of Hard-coded Password	1400	623
HasMember	B	260	Password in Configuration File	1400	629
HasMember	B	261	Weak Encoding for Password	1400	631
HasMember	B	262	Not Using Password Aging	1400	633
HasMember	B	263	Password Aging with Long Expiration	1400	636
HasMember	B	266	Incorrect Privilege Assignment	1400	638
HasMember	B	267	Privilege Defined With Unsafe Actions	1400	641
HasMember	B	268	Privilege Chaining	1400	644
HasMember	C	269	Improper Privilege Management	1400	646
HasMember	B	270	Privilege Context Switching Error	1400	651
HasMember	C	271	Privilege Dropping / Lowering Errors	1400	653
HasMember	B	272	Least Privilege Violation	1400	656
HasMember	B	273	Improper Check for Dropped Privileges	1400	660
HasMember	B	274	Improper Handling of Insufficient Privileges	1400	663
HasMember	B	276	Incorrect Default Permissions	1400	665
HasMember	V	277	Insecure Inherited Permissions	1400	668

Nature	Type	ID	Name	V	Page
HasMember	V	278	Insecure Preserved Inherited Permissions	1400	669
HasMember	V	279	Incorrect Execution-Assigned Permissions	1400	671
HasMember	B	280	Improper Handling of Insufficient Permissions or Privileges	1400	672
HasMember	B	281	Improper Preservation of Permissions	1400	674
HasMember	C	282	Improper Ownership Management	1400	676
HasMember	B	283	Unverified Ownership	1400	678
HasMember	P	284	Improper Access Control	1400	680
HasMember	C	285	Improper Authorization	1400	684
HasMember	C	286	Incorrect User Management	1400	691
HasMember	C	287	Improper Authentication	1400	692
HasMember	B	288	Authentication Bypass Using an Alternate Path or Channel	1400	700
HasMember	B	289	Authentication Bypass by Alternate Name	1400	703
HasMember	B	290	Authentication Bypass by Spoofing	1400	705
HasMember	V	291	Reliance on IP Address for Authentication	1400	708
HasMember	V	293	Using Referer Field for Authentication	1400	710
HasMember	B	294	Authentication Bypass by Capture-replay	1400	712
HasMember	B	295	Improper Certificate Validation	1400	714
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	1400	719
HasMember	V	297	Improper Validation of Certificate with Host Mismatch	1400	722
HasMember	V	298	Improper Validation of Certificate Expiration	1400	726
HasMember	B	299	Improper Check for Certificate Revocation	1400	727
HasMember	C	300	Channel Accessible by Non-Endpoint	1400	730
HasMember	B	301	Reflection Attack in an Authentication Protocol	1400	733
HasMember	B	302	Authentication Bypass by Assumed-Immutable Data	1400	735
HasMember	B	303	Incorrect Implementation of Authentication Algorithm	1400	737
HasMember	B	304	Missing Critical Step in Authentication	1400	738
HasMember	B	305	Authentication Bypass by Primary Weakness	1400	740
HasMember	B	306	Missing Authentication for Critical Function	1400	741
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	1400	747
HasMember	B	308	Use of Single-factor Authentication	1400	752
HasMember	B	309	Use of Password System for Primary Authentication	1400	754
HasMember	V	321	Use of Hard-coded Cryptographic Key	1400	785
HasMember	B	322	Key Exchange without Entity Authentication	1400	788
HasMember	V	350	Reliance on Reverse DNS Resolution for a Security-Critical Action	1400	863
HasMember	V	370	Missing Check for Certificate Revocation after Initial Check	1400	917
HasMember		384	Session Fixation	1400	936
HasMember	B	419	Unprotected Primary Channel	1400	1017
HasMember	B	420	Unprotected Alternate Channel	1400	1018
HasMember	B	421	Race Condition During Access to Alternate Channel	1400	1020
HasMember	V	422	Unprotected Windows Messaging Channel ('Shatter')	1400	1022
HasMember	B	425	Direct Request ('Forced Browsing')	1400	1025
HasMember	C	441	Unintended Proxy or Intermediary ('Confused Deputy')	1400	1064
HasMember	V	520	.NET Misconfiguration: Use of Impersonation	1400	1222
HasMember	B	521	Weak Password Requirements	1400	1223

Nature	Type	ID	Name	V	Page
HasMember	C	522	Insufficiently Protected Credentials	1400	1225
HasMember	B	523	Unprotected Transport of Credentials	1400	1230
HasMember	B	549	Missing Password Field Masking	1400	1262
HasMember	B	551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization	1400	1264
HasMember	V	555	J2EE Misconfiguration: Plaintext Password in Configuration File	1400	1270
HasMember	V	556	ASP.NET Misconfiguration: Use of Identity Impersonation	1400	1271
HasMember	V	566	Authorization Bypass Through User-Controlled SQL Primary Key	1400	1286
HasMember	V	593	Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created	1400	1331
HasMember	V	599	Missing Validation of OpenSSL Certificate	1400	1341
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1400	1345
HasMember	B	603	Use of Client-Side Authentication	1400	1354
HasMember	B	611	Improper Restriction of XML External Entity Reference	1400	1367
HasMember	B	612	Improper Authorization of Index Containing Sensitive Information	1400	1370
HasMember	B	613	Insufficient Session Expiration	1400	1371
HasMember	B	620	Unverified Password Change	1400	1383
HasMember	V	623	Unsafe ActiveX Control Marked Safe For Scripting	1400	1389
HasMember	B	639	Authorization Bypass Through User-Controlled Key	1400	1406
HasMember	B	640	Weak Password Recovery Mechanism for Forgotten Password	1400	1409
HasMember	B	645	Overly Restrictive Account Lockout Mechanism	1400	1423
HasMember	V	647	Use of Non-Canonical URL Paths for Authorization Decisions	1400	1426
HasMember	B	648	Incorrect Use of Privileged APIs	1400	1428
HasMember	B	708	Incorrect Ownership Assignment	1400	1548
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1400	1551
HasMember	B	798	Use of Hard-coded Credentials	1400	1690
HasMember	B	804	Guessable CAPTCHA	1400	1701
HasMember	B	836	Use of Password Hash Instead of Password for Authentication	1400	1761
HasMember	B	842	Placement of User into Incorrect Group	1400	1775
HasMember	C	862	Missing Authorization	1400	1780
HasMember	C	863	Incorrect Authorization	1400	1787
HasMember	B	918	Server-Side Request Forgery (SSRF)	1400	1820
HasMember	B	921	Storage of Sensitive Data in a Mechanism without Access Control	1400	1824
HasMember	C	923	Improper Restriction of Communication Channel to Intended Endpoints	1400	1827
HasMember	V	925	Improper Verification of Intent by Broadcast Receiver	1400	1831
HasMember	V	926	Improper Export of Android Application Components	1400	1833
HasMember	V	927	Use of Implicit Intent for Sensitive Communication	1400	1836
HasMember	B	939	Improper Authorization in Handler for Custom URL Scheme	1400	1840
HasMember	B	940	Improper Verification of Source of a Communication Channel	1400	1842

Nature	Type	ID	Name	V	Page
HasMember	B	941	Incorrectly Specified Destination in a Communication Channel	1400	1845
HasMember	V	942	Permissive Cross-domain Policy with Untrusted Domains	1400	1847
HasMember	V	1004	Sensitive Cookie Without 'HttpOnly' Flag	1400	1854
HasMember	B	1021	Improper Restriction of Rendered UI Layers or Frames	1400	1860
HasMember	V	1022	Use of Web Link to Untrusted Target with window.opener Access	1400	1862
HasMember	B	1191	On-Chip Debug and Test Interface With Improper Access Control	1400	1980
HasMember	B	1220	Insufficient Granularity of Access Control	1400	1992
HasMember	V	1222	Insufficient Granularity of Address Regions Protected by Register Locks	1400	1999
HasMember	B	1224	Improper Restriction of Write-Once Bit Fields	1400	2003
HasMember	B	1230	Exposure of Sensitive Information Through Metadata	1400	2006
HasMember	B	1231	Improper Prevention of Lock Bit Modification	1400	2007
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	1400	2012
HasMember	B	1242	Inclusion of Undocumented Features or Chicken Bits	1400	2033
HasMember	B	1243	Sensitive Non-Volatile Information Not Protected During Debug	1400	2035
HasMember	B	1244	Internal Asset Exposed to Unsafe Debug Access Level or State	1400	2037
HasMember	B	1252	CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations	1400	2056
HasMember	B	1256	Improper Restriction of Software Interfaces to Hardware Features	1400	2065
HasMember	B	1257	Improper Access Control Applied to Mirrored or Aliased Memory Regions	1400	2068
HasMember	B	1259	Improper Restriction of Security Token Assignment	1400	2073
HasMember	B	1260	Improper Handling of Overlap Between Protected Memory Ranges	1400	2075
HasMember	B	1262	Improper Access Control for Register Interface	1400	2081
HasMember	C	1263	Improper Physical Access Control	1400	2085
HasMember	B	1267	Policy Uses Obsolete Encoding	1400	2093
HasMember	B	1268	Policy Privileges are not Assigned Consistently Between Control and Data Agents	1400	2095
HasMember	B	1270	Generation of Incorrect Security Tokens	1400	2100
HasMember	B	1274	Improper Access Control for Volatile Memory Containing Boot Code	1400	2108
HasMember	V	1275	Sensitive Cookie with Improper SameSite Attribute	1400	2110
HasMember	B	1276	Hardware Child Block Incorrectly Connected to Parent System	1400	2113
HasMember	B	1283	Mutable Attestation or Measurement Reporting Data	1400	2128
HasMember	B	1290	Incorrect Decoding of Security Identifiers	1400	2142
HasMember	B	1292	Incorrect Conversion of Security Identifiers	1400	2147
HasMember	C	1294	Insecure Security Identifier Mechanism	1400	2150
HasMember	B	1296	Incorrect Chaining or Granularity of Debug Components	1400	2153
HasMember	B	1297	Unprotected Confidential Information on Device is Accessible by OSAT Vendors	1400	2156

Nature	Type	ID	Name	V	Page
HasMember	B	1299	Missing Protection Mechanism for Alternate Hardware Interface	1400	2162
HasMember	B	1302	Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC)	1400	2172
HasMember	B	1304	Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation	1400	2176
HasMember	B	1311	Improper Translation of Security Attributes by Fabric Bridge	1400	2182
HasMember	B	1312	Missing Protection for Mirrored Regions in On-Chip Fabric Firewall	1400	2184
HasMember	B	1313	Hardware Allows Activation of Test or Debug Logic at Runtime	1400	2185
HasMember	B	1314	Missing Write Protection for Parametric Data Values	1400	2187
HasMember	B	1315	Improper Setting of Bus Controlling Capability in Fabric End-point	1400	2190
HasMember	B	1316	Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges	1400	2192
HasMember	B	1317	Improper Access Control in Fabric Bridge	1400	2194
HasMember	B	1320	Improper Protection for Outbound Error Messages and Alert Signals	1400	2202
HasMember	B	1323	Improper Management of Sensitive Trace Data	1400	2208
HasMember	B	1328	Security Version Number Mutable to Older Versions	1400	2217
HasMember	B	1334	Unauthorized Error Injection Can Degrade Hardware Redundancy	1400	2234
HasMember	C	1390	Weak Authentication	1400	2267
HasMember	C	1391	Use of Weak Credentials	1400	2269
HasMember	B	1392	Use of Default Credentials	1400	2271
HasMember	B	1393	Use of Default Password	1400	2273
HasMember	B	1394	Use of Default Cryptographic Key	1400	2275

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	B	183	Permissive List of Allowed Inputs	1400	458
HasMember	C	185	Incorrect Regular Expression	1400	463
HasMember	B	186	Overly Restrictive Regular Expression	1400	466

Nature	Type	ID	Name	V	Page
HasMember	V	187	Partial String Comparison	1400	467
HasMember	B	478	Missing Default Case in Multiple Condition Expression	1400	1142
HasMember	V	486	Comparison of Classes by Name	1400	1164
HasMember	V	595	Comparison of Object References Instead of Object Contents	1400	1334
HasMember	V	597	Use of Wrong Operator in String Comparison	1400	1337
HasMember	B	625	Permissive Regular Expression	1400	1392
HasMember	P	697	Incorrect Comparison	1400	1530
HasMember	V	777	Regular Expression without Anchors	1400	1636
HasMember	B	839	Numeric Range Comparison Without Minimum Check	1400	1767
HasMember	C	1023	Incomplete Comparison with Missing Factors	1400	1865
HasMember	B	1024	Comparison of Incompatible Types	1400	1867
HasMember	B	1025	Comparison Using Wrong Factors	1400	1868
HasMember	V	1077	Floating Point Comparison with Incorrect Operator	1400	1917

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	V	14	Compiler Removal of Code to Clear Buffers	1400	14
HasMember	B	115	Misinterpretation of Input	1400	280
HasMember	P	435	Improper Interaction Between Multiple Correctly-Behaving Entities	1400	1055
HasMember	C	436	Interpretation Conflict	1400	1057
HasMember	B	437	Incomplete Model of Endpoint Features	1400	1059
HasMember	B	439	Behavioral Change in New Version or Environment	1400	1061
HasMember	B	444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	1400	1068
HasMember	V	650	Trusting HTTP Permission Methods on the Server Side	1400	1432
HasMember	B	733	Compiler Optimization Removal or Modification of Security-critical Code	1400	1562
HasMember	B	1037	Processor Optimization Removal or Modification of Security-critical Code	1400	1870
HasMember	C	1038	Insecure Automated Optimizations	1400	1872

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1400	293
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	1400	304
HasMember	V	121	Stack-based Buffer Overflow	1400	314
HasMember	V	122	Heap-based Buffer Overflow	1400	318
HasMember	B	123	Write-what-where Condition	1400	323
HasMember	B	124	Buffer Underwrite ('Buffer Underflow')	1400	326
HasMember	B	125	Out-of-bounds Read	1400	330
HasMember	V	126	Buffer Over-read	1400	334
HasMember	V	127	Buffer Under-read	1400	337
HasMember	V	129	Improper Validation of Array Index	1400	341
HasMember	B	131	Incorrect Calculation of Buffer Size	1400	355
HasMember	B	134	Use of Externally-Controlled Format String	1400	365
HasMember	B	188	Reliance on Data/Memory Layout	1400	470
HasMember	V	198	Use of Incorrect Byte Ordering	1400	503
HasMember	V	244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	1400	591
HasMember	V	401	Missing Release of Memory after Effective Lifetime	1400	973
HasMember	V	415	Double Free	1400	1008
HasMember	V	416	Use After Free	1400	1012
HasMember	B	466	Return of Pointer Value Outside of Expected Range	1400	1109
HasMember	B	562	Return of Stack Variable Address	1400	1278
HasMember	V	587	Assignment of a Fixed Address to a Pointer	1400	1322
HasMember	V	590	Free of Memory not on the Heap	1400	1326
HasMember	∞	680	Integer Overflow to Buffer Overflow	1400	1493
HasMember	∞	690	Unchecked Return Value to NULL Pointer Dereference	1400	1514
HasMember	V	761	Free of Pointer not at Start of Buffer	1400	1592
HasMember	V	762	Mismatched Memory Management Routines	1400	1596
HasMember	B	763	Release of Invalid Pointer or Reference	1400	1599
HasMember	B	786	Access of Memory Location Before Start of Buffer	1400	1658
HasMember	B	787	Out-of-bounds Write	1400	1661
HasMember	B	788	Access of Memory Location After End of Buffer	1400	1669
HasMember	V	789	Memory Allocation with Excessive Size Value	1400	1674
HasMember	B	805	Buffer Access with Incorrect Length Value	1400	1702
HasMember	V	806	Buffer Access Using Size of Source Buffer	1400	1710
HasMember	B	822	Untrusted Pointer Dereference	1400	1723
HasMember	B	823	Use of Out-of-range Pointer Offset	1400	1726
HasMember	B	824	Access of Uninitialized Pointer	1400	1729
HasMember	B	825	Expired Pointer Dereference	1400	1732

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 >.

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	2598
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	1400	888
HasMember	B	363	Race Condition Enabling Link Following	1400	897
HasMember	B	364	Signal Handler Race Condition	1400	899
HasMember	B	366	Race Condition within a Thread	1400	904
HasMember	B	367	Time-of-check Time-of-use (TOCTOU) Race Condition	1400	906
HasMember	B	368	Context Switching Race Condition	1400	912
HasMember	B	412	Unrestricted Externally Accessible Lock	1400	1000
HasMember	B	413	Improper Resource Locking	1400	1003
HasMember	B	414	Missing Lock Check	1400	1007
HasMember	B	432	Dangerous Signal Handler not Disabled During Sensitive Operations	1400	1045
HasMember	V	479	Signal Handler Use of a Non-reentrant Function	1400	1147
HasMember	V	543	Use of Singleton Pattern Without Synchronization in a Multithreaded Context	1400	1255
HasMember	V	558	Use of getlogin() in Multithreaded Application	1400	1272
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	1400	1288
HasMember	V	572	Call to Thread run() instead of start()	1400	1296
HasMember	V	574	EJB Bad Practices: Use of Synchronization Primitives	1400	1300
HasMember	V	591	Sensitive Data Storage in Improperly Locked Memory	1400	1329
HasMember	B	609	Double-Checked Locking	1400	1362
HasMember	B	663	Use of a Non-reentrant Function in a Concurrent Context	1400	1452
HasMember	C	667	Improper Locking	1400	1464
HasMember	♣	689	Permission Race Condition During Resource Copy	1400	1513
HasMember	B	764	Multiple Locks of a Critical Resource	1400	1604
HasMember	B	765	Multiple Unlocks of a Critical Resource	1400	1605
HasMember	B	820	Missing Synchronization	1400	1720
HasMember	B	821	Incorrect Synchronization	1400	1722

Nature	Type	ID	Name	V	Page
HasMember	V	828	Signal Handler with Functionality that is not Asynchronous-Safe	1400	1737
HasMember	V	831	Signal Handler Function Associated with Multiple Signals	1400	1749
HasMember	B	832	Unlock of a Resource that is not Locked	1400	1752
HasMember	B	833	Deadlock	1400	1753
HasMember	B	1058	Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element	1400	1893
HasMember	B	1088	Synchronous Access of Remote Resource without Timeout	1400	1928
HasMember	V	1096	Singleton Class Instance Creation without Proper Locking or Synchronization	1400	1936
HasMember	B	1223	Race Condition for Write-Once Attributes	1400	2001
HasMember	B	1232	Improper Lock Behavior After Power State Transition	1400	2010
HasMember	B	1234	Hardware Internal or Debug Modes Allow Override of Locks	1400	2014
HasMember	B	1264	Hardware Logic with Insecure De-Synchronization between Control and Data Channels	1400	2086
HasMember	B	1298	Hardware Logic Contains Race Conditions	1400	2158

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	V	5	J2EE Misconfiguration: Data Transmission Without Encryption	1400	1
HasMember	C	311	Missing Encryption of Sensitive Data	1400	757
HasMember	B	312	Cleartext Storage of Sensitive Information	1400	764
HasMember	V	313	Cleartext Storage in a File or on Disk	1400	770
HasMember	V	314	Cleartext Storage in the Registry	1400	772
HasMember	V	315	Cleartext Storage of Sensitive Information in a Cookie	1400	774
HasMember	V	316	Cleartext Storage of Sensitive Information in Memory	1400	775
HasMember	V	317	Cleartext Storage of Sensitive Information in GUI	1400	777
HasMember	V	318	Cleartext Storage of Sensitive Information in Executable	1400	778
HasMember	B	319	Cleartext Transmission of Sensitive Information	1400	779
HasMember	B	324	Use of a Key Past its Expiration Date	1400	792
HasMember	B	325	Missing Cryptographic Step	1400	794
HasMember	C	326	Inadequate Encryption Strength	1400	796
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	1400	799

Nature	Type	ID	Name	V	Page
HasMember	B	328	Use of Weak Hash	1400	806
HasMember	B	347	Improper Verification of Cryptographic Signature	1400	857
HasMember	V	614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	1400	1373
HasMember	V	759	Use of a One-Way Hash without a Salt	1400	1585
HasMember	V	760	Use of a One-Way Hash with a Predictable Salt	1400	1589
HasMember	V	780	Use of RSA Algorithm without OAEP	1400	1644
HasMember	B	916	Use of Password Hash With Insufficient Computational Effort	1400	1813
HasMember	B	1240	Use of a Cryptographic Primitive with a Risky Implementation	1400	2025

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
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	132
HasMember	C	114	Process Control	1400	277
HasMember	V	219	Storage of File with Sensitive Data Under Web Root	1400	553
HasMember	V	220	Storage of File With Sensitive Data Under FTP Root	1400	555
HasMember	B	374	Passing Mutable Objects to an Untrusted Method	1400	920
HasMember	B	375	Returning a Mutable Object to an Untrusted Caller	1400	923
HasMember	C	377	Insecure Temporary File	1400	925
HasMember	B	378	Creation of Temporary File With Insecure Permissions	1400	928
HasMember	B	379	Creation of Temporary File in Directory with Insecure Permissions	1400	930
HasMember	C	402	Transmission of Private Resources into a New Sphere ('Resource Leak')	1400	976
HasMember	B	403	Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak')	1400	978
HasMember	B	426	Untrusted Search Path	1400	1028
HasMember	B	427	Uncontrolled Search Path Element	1400	1033
HasMember	B	428	Unquoted Search Path or Element	1400	1039
HasMember	V	433	Unparsed Raw Web Content Delivery	1400	1046
HasMember	B	472	External Control of Assumed-Immutable Web Parameter	1400	1123
HasMember	B	488	Exposure of Data Element to Wrong Session	1400	1169

Nature	Type	ID	Name	V	Page
HasMember	V	491	Public cloneable() Method Without Final ('Object Hijack')	1400	1174
HasMember	V	492	Use of Inner Class Containing Sensitive Data	1400	1175
HasMember	V	493	Critical Public Variable Without Final Modifier	1400	1182
HasMember	V	498	Cloneable Class Containing Sensitive Information	1400	1196
HasMember	V	499	Serializable Class Containing Sensitive Data	1400	1198
HasMember	V	500	Public Static Field Not Marked Final	1400	1200
HasMember	B	524	Use of Cache Containing Sensitive Information	1400	1232
HasMember	V	525	Use of Web Browser Cache Containing Sensitive Information	1400	1233
HasMember	V	527	Exposure of Version-Control Repository to an Unauthorized Control Sphere	1400	1236
HasMember	V	528	Exposure of Core Dump File to an Unauthorized Control Sphere	1400	1237
HasMember	V	529	Exposure of Access Control List Files to an Unauthorized Control Sphere	1400	1238
HasMember	V	530	Exposure of Backup File to an Unauthorized Control Sphere	1400	1239
HasMember	V	539	Use of Persistent Cookies Containing Sensitive Information	1400	1250
HasMember	B	552	Files or Directories Accessible to External Parties	1400	1265
HasMember	V	553	Command Shell in Externally Accessible Directory	1400	1269
HasMember	B	565	Reliance on Cookies without Validation and Integrity Checking	1400	1283
HasMember	V	582	Array Declared Public, Final, and Static	1400	1314
HasMember	V	583	finalize() Method Declared Public	1400	1315
HasMember	V	608	Struts: Non-private Field in ActionForm Class	1400	1361
HasMember	B	619	Dangling Database Cursor ('Cursor Injection')	1400	1382
HasMember	C	642	External Control of Critical State Data	1400	1414
HasMember	C	668	Exposure of Resource to Wrong Sphere	1400	1469
HasMember	B	767	Access to Critical Private Variable via Public Method	1400	1610
HasMember	V	784	Reliance on Cookies without Validation and Integrity Checking in a Security Decision	1400	1653
HasMember	B	1282	Assumed-Immutable Data is Stored in Writable Memory	1400	2127
HasMember	B	1327	Binding to an Unrestricted IP Address	1400	2215

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598

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	54
HasMember	V	26	Path Traversal: '/dir/../filename'	1400	56
HasMember	V	27	Path Traversal: 'dir/../../filename'	1400	58
HasMember	V	28	Path Traversal: '..\filedir'	1400	59
HasMember	V	29	Path Traversal: '\..\filename'	1400	61
HasMember	V	30	Path Traversal: '\dir\..\filename'	1400	63
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	80
HasMember	V	39	Path Traversal: 'C:dirname'	1400	82
HasMember	V	40	Path Traversal: '\\UNC\share\name\' (Windows UNC Share)	1400	85
HasMember	B	41	Improper Resolution of Path Equivalence	1400	86
HasMember	V	42	Path Equivalence: 'filename.' (Trailing Dot)	1400	92
HasMember	V	43	Path Equivalence: 'filename....' (Multiple Trailing Dot)	1400	93
HasMember	V	44	Path Equivalence: 'file.name' (Internal Dot)	1400	94
HasMember	V	45	Path Equivalence: 'file...name' (Multiple Internal Dot)	1400	95
HasMember	V	46	Path Equivalence: 'filename ' (Trailing Space)	1400	96
HasMember	V	47	Path Equivalence: ' filename' (Leading Space)	1400	97
HasMember	V	48	Path Equivalence: 'file name' (Internal Whitespace)	1400	98
HasMember	V	49	Path Equivalence: 'filename/' (Trailing Slash)	1400	99
HasMember	V	50	Path Equivalence: '//multiple/leading/slash'	1400	100
HasMember	V	51	Path Equivalence: '/multiple//internal/slash'	1400	102
HasMember	V	52	Path Equivalence: '/multiple/trailing/slash//'	1400	103
HasMember	V	53	Path Equivalence: '\multiple\\internal\backslash'	1400	104
HasMember	V	54	Path Equivalence: 'filedir\' (Trailing Backslash)	1400	105
HasMember	V	55	Path Equivalence: '/./' (Single Dot Directory)	1400	106
HasMember	V	56	Path Equivalence: 'filedir*' (Wildcard)	1400	107
HasMember	V	57	Path Equivalence: 'fakedir/../realdir/filename'	1400	108
HasMember	V	58	Path Equivalence: Windows 8.3 Filename	1400	110
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	1400	111
HasMember	C	61	UNIX Symbolic Link (Symlink) Following	1400	116
HasMember	V	62	UNIX Hard Link	1400	119
HasMember	V	64	Windows Shortcut Following (.LNK)	1400	121
HasMember	V	65	Windows Hard Link	1400	123
HasMember	B	66	Improper Handling of File Names that Identify Virtual Resources	1400	124
HasMember	V	67	Improper Handling of Windows Device Names	1400	126

Nature	Type	ID	Name	V	Page
HasMember	V	69	Improper Handling of Windows ::DATA Alternate Data Stream	1400	129
HasMember	V	72	Improper Handling of Apple HFS+ Alternate Data Stream Path	1400	130

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
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	606
HasMember	B	390	Detection of Error Condition Without Action	1400	943
HasMember	B	391	Unchecked Error Condition	1400	948
HasMember	B	394	Unexpected Status Code or Return Value	1400	955
HasMember	B	544	Missing Standardized Error Handling Mechanism	1400	1256
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1400	1535
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1400	1568
HasMember	C	755	Improper Handling of Exceptional Conditions	1400	1576
HasMember	B	756	Missing Custom Error Page	1400	1579
HasMember	B	1247	Improper Protection Against Voltage and Clock Glitches	1400	2044
HasMember	B	1261	Improper Handling of Single Event Upsets	1400	2079
HasMember	B	1332	Improper Handling of Faults that Lead to Instruction Skips	1400	2227
HasMember	B	1351	Improper Handling of Hardware Behavior in Exceptionally Cold Environments	1400	2252
HasMember	C	1384	Improper Handling of Physical or Environmental Conditions	1400	2257

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	C	20	Improper Input Validation	1400	20
HasMember	V	105	Struts: Form Field Without Validator	1400	253
HasMember	V	106	Struts: Plug-in Framework not in Use	1400	256
HasMember	V	108	Struts: Unvalidated Action Form	1400	261
HasMember	V	109	Struts: Validator Turned Off	1400	263
HasMember	B	112	Missing XML Validation	1400	269
HasMember	V	554	ASP.NET Misconfiguration: Not Using Input Validation Framework	1400	1269
HasMember	B	606	Unchecked Input for Loop Condition	1400	1357
HasMember	V	622	Improper Validation of Function Hook Arguments	1400	1387
HasMember	V	781	Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code	1400	1646
HasMember	B	1173	Improper Use of Validation Framework	1400	1969
HasMember	V	1174	ASP.NET Misconfiguration: Improper Model Validation	1400	1970
HasMember	B	1284	Improper Validation of Specified Quantity in Input	1400	2130
HasMember	B	1285	Improper Validation of Specified Index, Position, or Offset in Input	1400	2132
HasMember	B	1286	Improper Validation of Syntactic Correctness of Input	1400	2136
HasMember	B	1287	Improper Validation of Specified Type of Input	1400	2138
HasMember	B	1288	Improper Validation of Consistency within Input	1400	2139
HasMember	B	1289	Improper Validation of Unsafe Equivalence in Input	1400	2141

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	C	116	Improper Encoding or Escaping of Output	1400	281
HasMember	B	117	Improper Output Neutralization for Logs	1400	288
HasMember	B	130	Improper Handling of Length Parameter Inconsistency	1400	351
HasMember	C	138	Improper Neutralization of Special Elements	1400	373
HasMember	B	140	Improper Neutralization of Delimiters	1400	376
HasMember	V	141	Improper Neutralization of Parameter/Argument Delimiters	1400	378

Nature	Type	ID	Name	V	Page
HasMember	V	142	Improper Neutralization of Value Delimiters	1400	380
HasMember	V	143	Improper Neutralization of Record Delimiters	1400	381
HasMember	V	144	Improper Neutralization of Line Delimiters	1400	383
HasMember	V	145	Improper Neutralization of Section Delimiters	1400	385
HasMember	V	146	Improper Neutralization of Expression/Command Delimiters	1400	387
HasMember	V	147	Improper Neutralization of Input Terminators	1400	389
HasMember	V	148	Improper Neutralization of Input Leaders	1400	391
HasMember	V	149	Improper Neutralization of Quoting Syntax	1400	392
HasMember	V	150	Improper Neutralization of Escape, Meta, or Control Sequences	1400	394
HasMember	V	151	Improper Neutralization of Comment Delimiters	1400	396
HasMember	V	152	Improper Neutralization of Macro Symbols	1400	398
HasMember	V	153	Improper Neutralization of Substitution Characters	1400	400
HasMember	V	154	Improper Neutralization of Variable Name Delimiters	1400	401
HasMember	V	155	Improper Neutralization of Wildcards or Matching Symbols	1400	403
HasMember	V	156	Improper Neutralization of Whitespace	1400	405
HasMember	V	157	Failure to Sanitize Paired Delimiters	1400	407
HasMember	V	158	Improper Neutralization of Null Byte or NUL Character	1400	409
HasMember	C	159	Improper Handling of Invalid Use of Special Elements	1400	411
HasMember	V	160	Improper Neutralization of Leading Special Elements	1400	413
HasMember	V	161	Improper Neutralization of Multiple Leading Special Elements	1400	415
HasMember	V	162	Improper Neutralization of Trailing Special Elements	1400	417
HasMember	V	163	Improper Neutralization of Multiple Trailing Special Elements	1400	418
HasMember	V	164	Improper Neutralization of Internal Special Elements	1400	420
HasMember	V	165	Improper Neutralization of Multiple Internal Special Elements	1400	422
HasMember	B	166	Improper Handling of Missing Special Element	1400	423
HasMember	B	167	Improper Handling of Additional Special Element	1400	425
HasMember	B	168	Improper Handling of Inconsistent Special Elements	1400	426
HasMember	B	170	Improper Null Termination	1400	428
HasMember	C	172	Encoding Error	1400	433
HasMember	V	173	Improper Handling of Alternate Encoding	1400	435
HasMember	V	174	Double Decoding of the Same Data	1400	437
HasMember	V	175	Improper Handling of Mixed Encoding	1400	439
HasMember	V	176	Improper Handling of Unicode Encoding	1400	440
HasMember	V	177	Improper Handling of URL Encoding (Hex Encoding)	1400	442
HasMember	C	228	Improper Handling of Syntactically Invalid Structure	1400	568
HasMember	B	229	Improper Handling of Values	1400	570
HasMember	V	230	Improper Handling of Missing Values	1400	570
HasMember	V	231	Improper Handling of Extra Values	1400	572
HasMember	V	232	Improper Handling of Undefined Values	1400	573
HasMember	B	233	Improper Handling of Parameters	1400	574
HasMember	V	234	Failure to Handle Missing Parameter	1400	576
HasMember	V	235	Improper Handling of Extra Parameters	1400	578
HasMember	V	236	Improper Handling of Undefined Parameters	1400	579

Nature	Type	ID	Name	V	Page
HasMember	B	237	Improper Handling of Structural Elements	1400	580
HasMember	V	238	Improper Handling of Incomplete Structural Elements	1400	581
HasMember	V	239	Failure to Handle Incomplete Element	1400	582
HasMember	B	240	Improper Handling of Inconsistent Structural Elements	1400	583
HasMember	B	241	Improper Handling of Unexpected Data Type	1400	584
HasMember	B	463	Deletion of Data Structure Sentinel	1400	1105
HasMember	B	464	Addition of Data Structure Sentinel	1400	1107
HasMember	V	626	Null Byte Interaction Error (Poison Null Byte)	1400	1394
HasMember	V	644	Improper Neutralization of HTTP Headers for Scripting Syntax	1400	1422
HasMember	P	707	Improper Neutralization	1400	1546
HasMember	C	790	Improper Filtering of Special Elements	1400	1678
HasMember	B	791	Incomplete Filtering of Special Elements	1400	1680
HasMember	V	792	Incomplete Filtering of One or More Instances of Special Elements	1400	1681
HasMember	V	793	Only Filtering One Instance of a Special Element	1400	1683
HasMember	V	794	Incomplete Filtering of Multiple Instances of Special Elements	1400	1684
HasMember	B	795	Only Filtering Special Elements at a Specified Location	1400	1685
HasMember	V	796	Only Filtering Special Elements Relative to a Marker	1400	1687
HasMember	V	797	Only Filtering Special Elements at an Absolute Position	1400	1689
HasMember	B	838	Inappropriate Encoding for Output Context	1400	1764

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	B	128	Wrap-around Error	1400	339
HasMember	B	135	Incorrect Calculation of Multi-Byte String Length	1400	370
HasMember	B	190	Integer Overflow or Wraparound	1400	472
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	1400	480
HasMember	B	193	Off-by-one Error	1400	486
HasMember	B	369	Divide By Zero	1400	913
HasMember	V	467	Use of sizeof() on a Pointer Type	1400	1110
HasMember	B	468	Incorrect Pointer Scaling	1400	1114
HasMember	B	469	Use of Pointer Subtraction to Determine Size	1400	1115
HasMember	P	682	Incorrect Calculation	1400	1499
HasMember	B	1335	Incorrect Bitwise Shift of Integer	1400	2235

Nature	Type	ID	Name	V	Page
HasMember	B	1339	Insufficient Precision or Accuracy of a Real Number	1400	2242

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	1400	137
HasMember	C	75	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)	1400	142
HasMember	B	76	Improper Neutralization of Equivalent Special Elements	1400	144
HasMember	C	77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	1400	145
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	1400	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	1400	163
HasMember	V	80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	1400	177
HasMember	V	81	Improper Neutralization of Script in an Error Message Web Page	1400	179
HasMember	V	82	Improper Neutralization of Script in Attributes of IMG Tags in a Web Page	1400	182
HasMember	V	83	Improper Neutralization of Script in Attributes in a Web Page	1400	183
HasMember	V	84	Improper Neutralization of Encoded URI Schemes in a Web Page	1400	186
HasMember	V	85	Doubled Character XSS Manipulations	1400	188
HasMember	V	86	Improper Neutralization of Invalid Characters in Identifiers in Web Pages	1400	190
HasMember	V	87	Improper Neutralization of Alternate XSS Syntax	1400	192
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	1400	194
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	1400	201
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	1400	212
HasMember	B	91	XML Injection (aka Blind XPath Injection)	1400	215
HasMember	B	93	Improper Neutralization of CRLF Sequences ('CRLF Injection')	1400	217

Nature	Type	ID	Name	V	Page
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	1400	219
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	1400	226
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	1400	232
HasMember	V	97	Improper Neutralization of Server-Side Includes (SSI) Within a Web Page	1400	235
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	1400	243
HasMember	V	102	Struts: Duplicate Validation Forms	1400	246
HasMember	V	113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')	1400	271
HasMember	V	564	SQL Injection: Hibernate	1400	1282
HasMember	V	621	Variable Extraction Error	1400	1385
HasMember	B	624	Executable Regular Expression Error	1400	1390
HasMember	V	627	Dynamic Variable Evaluation	1400	1396
HasMember	B	641	Improper Restriction of Names for Files and Other Resources	1400	1412
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1400	1419
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1400	1435
HasMember	∞	692	Incomplete Denylist to Cross-Site Scripting	1400	1519
HasMember	B	694	Use of Multiple Resources with Duplicate Identifier	1400	1523
HasMember	B	914	Improper Control of Dynamically-Identified Variables	1400	1807
HasMember	B	917	Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection')	1400	1818
HasMember	C	943	Improper Neutralization of Special Elements in Data Query Logic	1400	1850
HasMember	B	1236	Improper Neutralization of Formula Elements in a CSV File	1400	2019
HasMember	B	1336	Improper Neutralization of Special Elements Used in a Template Engine	1400	2238

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	B	179	Incorrect Behavior Order: Early Validation	1400	448
HasMember	V	180	Incorrect Behavior Order: Validate Before Canonicalize	1400	451
HasMember	V	181	Incorrect Behavior Order: Validate Before Filter	1400	453
HasMember	B	248	Uncaught Exception	1400	596
HasMember	V	382	J2EE Bad Practices: Use of System.exit()	1400	933
HasMember	B	395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	1400	957
HasMember	B	396	Declaration of Catch for Generic Exception	1400	959
HasMember	B	397	Declaration of Throws for Generic Exception	1400	961
HasMember	B	408	Incorrect Behavior Order: Early Amplification	1400	995
HasMember	B	430	Deployment of Wrong Handler	1400	1042
HasMember	B	431	Missing Handler	1400	1043
HasMember	B	455	Non-exit on Failed Initialization	1400	1087
HasMember	B	480	Use of Incorrect Operator	1400	1150
HasMember	V	481	Assigning instead of Comparing	1400	1154
HasMember	V	482	Comparing instead of Assigning	1400	1157
HasMember	B	483	Incorrect Block Delimitation	1400	1160
HasMember	B	584	Return Inside Finally Block	1400	1317
HasMember	V	600	Uncaught Exception in Servlet	1400	1343
HasMember	B	617	Reachable Assertion	1400	1378
HasMember	C	670	Always-Incorrect Control Flow Implementation	1400	1475
HasMember	C	674	Uncontrolled Recursion	1400	1484
HasMember	P	691	Insufficient Control Flow Management	1400	1517
HasMember	C	696	Incorrect Behavior Order	1400	1527
HasMember	B	698	Execution After Redirect (EAR)	1400	1533
HasMember	C	705	Incorrect Control Flow Scoping	1400	1542
HasMember	V	768	Incorrect Short Circuit Evaluation	1400	1612
HasMember	B	783	Operator Precedence Logic Error	1400	1650
HasMember	C	799	Improper Control of Interaction Frequency	1400	1699
HasMember	C	834	Excessive Iteration	1400	1754
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1400	1757
HasMember	B	837	Improper Enforcement of a Single, Unique Action	1400	1762
HasMember	B	841	Improper Enforcement of Behavioral Workflow	1400	1772
HasMember	B	1190	DMA Device Enabled Too Early in Boot Phase	1400	1978
HasMember	B	1193	Power-On of Untrusted Execution Core Before Enabling Fabric Access Control	1400	1986
HasMember	B	1265	Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls	1400	2088
HasMember	B	1280	Access Control Check Implemented After Asset is Accessed	1400	2122
HasMember	B	1281	Sequence of Processor Instructions Leads to Unexpected Behavior	1400	2124
HasMember	B	1322	Use of Blocking Code in Single-threaded, Non-blocking Context	1400	2207

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	C	345	Insufficient Verification of Data Authenticity	1400	851
HasMember	C	346	Origin Validation Error	1400	853
HasMember	B	348	Use of Less Trusted Source	1400	859
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	1400	861
HasMember	B	351	Insufficient Type Distinction	1400	866
HasMember	A	352	Cross-Site Request Forgery (CSRF)	1400	868
HasMember	B	353	Missing Support for Integrity Check	1400	874
HasMember	B	354	Improper Validation of Integrity Check Value	1400	876
HasMember	B	360	Trust of System Event Data	1400	887
HasMember	B	494	Download of Code Without Integrity Check	1400	1185
HasMember	V	616	Incomplete Identification of Uploaded File Variables (PHP)	1400	1376
HasMember	V	646	Reliance on File Name or Extension of Externally-Supplied File	1400	1425
HasMember	B	649	Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking	1400	1430
HasMember	B	924	Improper Enforcement of Message Integrity During Transmission in a Communication Channel	1400	1830
HasMember	B	1293	Missing Source Correlation of Multiple Independent Data	1400	2149
HasMember	V	1385	Missing Origin Validation in WebSockets	1400	2259

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	V	11	ASP.NET Misconfiguration: Creating Debug Binary	1400	9
HasMember	V	103	Struts: Incomplete validate() Method Definition	1400	248

Nature	Type	ID	Name	V	Page
HasMember	V	104	Struts: Form Bean Does Not Extend Validation Class	1400	251
HasMember	V	107	Struts: Unused Validation Form	1400	259
HasMember	V	110	Struts: Validator Without Form Field	1400	264
HasMember	V	111	Direct Use of Unsafe JNI	1400	266
HasMember	B	242	Use of Inherently Dangerous Function	1400	586
HasMember	V	245	J2EE Bad Practices: Direct Management of Connections	1400	592
HasMember	V	246	J2EE Bad Practices: Direct Use of Sockets	1400	594
HasMember	B	253	Incorrect Check of Function Return Value	1400	613
HasMember	B	358	Improperly Implemented Security Check for Standard	1400	881
HasMember	V	383	J2EE Bad Practices: Direct Use of Threads	1400	935
HasMember	B	392	Missing Report of Error Condition	1400	951
HasMember	B	393	Return of Wrong Status Code	1400	953
HasMember	B	440	Expected Behavior Violation	1400	1062
HasMember	C	446	UI Discrepancy for Security Feature	1400	1073
HasMember	B	448	Obsolete Feature in UI	1400	1076
HasMember	B	449	The UI Performs the Wrong Action	1400	1077
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1400	1079
HasMember	V	462	Duplicate Key in Associative List (Alist)	1400	1104
HasMember	B	474	Use of Function with Inconsistent Implementations	1400	1128
HasMember	B	475	Undefined Behavior for Input to API	1400	1130
HasMember	B	476	NULL Pointer Dereference	1400	1132
HasMember	B	477	Use of Obsolete Function	1400	1138
HasMember	B	484	Omitted Break Statement in Switch	1400	1162
HasMember	B	489	Active Debug Code	1400	1171
HasMember	C	506	Embedded Malicious Code	1400	1210
HasMember	B	507	Trojan Horse	1400	1212
HasMember	B	508	Non-Replicating Malicious Code	1400	1213
HasMember	B	509	Replicating Malicious Code (Virus or Worm)	1400	1214
HasMember	B	510	Trapdoor	1400	1215
HasMember	B	511	Logic/Time Bomb	1400	1216
HasMember	B	512	Spyware	1400	1218
HasMember	V	546	Suspicious Comment	1400	1258
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	1400	1259
HasMember	V	560	Use of umask() with chmod-style Argument	1400	1274
HasMember	B	561	Dead Code	1400	1275
HasMember	B	563	Assignment to Variable without Use	1400	1280
HasMember	B	570	Expression is Always False	1400	1292
HasMember	B	571	Expression is Always True	1400	1295
HasMember	C	573	Improper Following of Specification by Caller	1400	1298
HasMember	V	575	EJB Bad Practices: Use of AWT Swing	1400	1301
HasMember	V	576	EJB Bad Practices: Use of Java I/O	1400	1304
HasMember	V	577	EJB Bad Practices: Use of Sockets	1400	1305
HasMember	V	578	EJB Bad Practices: Use of Class Loader	1400	1307
HasMember	V	579	J2EE Bad Practices: Non-serializable Object Stored in Session	1400	1309
HasMember	V	581	Object Model Violation: Just One of Equals and Hashcode Defined	1400	1312

Nature	Type	ID	Name	V	Page
HasMember	V	585	Empty Synchronized Block	1400	1318
HasMember	B	586	Explicit Call to Finalize()	1400	1320
HasMember	V	589	Call to Non-ubiquitous API	1400	1325
HasMember	V	594	J2EE Framework: Saving Unserializable Objects to Disk	1400	1332
HasMember	V	605	Multiple Binds to the Same Port	1400	1356
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1400	1398
HasMember	C	675	Multiple Operations on Resource in Single-Operation Context	1400	1487
HasMember	B	676	Use of Potentially Dangerous Function	1400	1489
HasMember	V	683	Function Call With Incorrect Order of Arguments	1400	1504
HasMember	C	684	Incorrect Provision of Specified Functionality	1400	1505
HasMember	V	685	Function Call With Incorrect Number of Arguments	1400	1507
HasMember	V	686	Function Call With Incorrect Argument Type	1400	1508
HasMember	V	687	Function Call With Incorrectly Specified Argument Value	1400	1510
HasMember	V	688	Function Call With Incorrect Variable or Reference as Argument	1400	1511
HasMember	B	695	Use of Low-Level Functionality	1400	1524
HasMember	P	710	Improper Adherence to Coding Standards	1400	1549
HasMember	C	758	Reliance on Undefined, Unspecified, or Implementation-Defined Behavior	1400	1582
HasMember	B	766	Critical Data Element Declared Public	1400	1607
HasMember	V	785	Use of Path Manipulation Function without Maximum-sized Buffer	1400	1656
HasMember	C	912	Hidden Functionality	1400	1803
HasMember	B	1007	Insufficient Visual Distinction of Homoglyphs Presented to User	1400	1857
HasMember	B	1041	Use of Redundant Code	1400	1875
HasMember	B	1043	Data Element Aggregating an Excessively Large Number of Non-Primitive Elements	1400	1877
HasMember	B	1044	Architecture with Number of Horizontal Layers Outside of Expected Range	1400	1879
HasMember	B	1045	Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor	1400	1880
HasMember	B	1047	Modules with Circular Dependencies	1400	1882
HasMember	B	1048	Invokable Control Element with Large Number of Outward Calls	1400	1883
HasMember	B	1053	Missing Documentation for Design	1400	1888
HasMember	B	1054	Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer	1400	1889
HasMember	B	1055	Multiple Inheritance from Concrete Classes	1400	1890
HasMember	B	1056	Invokable Control Element with Variadic Parameters	1400	1891
HasMember	B	1057	Data Access Operations Outside of Expected Data Manager Component	1400	1892
HasMember	C	1059	Insufficient Technical Documentation	1400	1894
HasMember	B	1060	Excessive Number of Inefficient Server-Side Data Accesses	1400	1897
HasMember	C	1061	Insufficient Encapsulation	1400	1898
HasMember	B	1062	Parent Class with References to Child Class	1400	1900
HasMember	B	1064	Invokable Control Element with Signature Containing an Excessive Number of Parameters	1400	1902

Nature	Type	ID	Name	V	Page
HasMember	B	1065	Runtime Resource Management Control Element in a Component Built to Run on Application Servers	1400	1903
HasMember	B	1066	Missing Serialization Control Element	1400	1904
HasMember	B	1068	Inconsistency Between Implementation and Documented Design	1400	1906
HasMember	V	1069	Empty Exception Block	1400	1907
HasMember	B	1070	Serializable Data Element Containing non-Serializable Item Elements	1400	1909
HasMember	B	1071	Empty Code Block	1400	1910
HasMember	B	1074	Class with Excessively Deep Inheritance	1400	1914
HasMember	B	1075	Unconditional Control Flow Transfer outside of Switch Block	1400	1915
HasMember	C	1076	Insufficient Adherence to Expected Conventions	1400	1916
HasMember	C	1078	Inappropriate Source Code Style or Formatting	1400	1918
HasMember	B	1079	Parent Class without Virtual Destructor Method	1400	1919
HasMember	B	1080	Source Code File with Excessive Number of Lines of Code	1400	1920
HasMember	B	1082	Class Instance Self Destruction Control Element	1400	1921
HasMember	B	1083	Data Access from Outside Expected Data Manager Component	1400	1922
HasMember	B	1085	Invokable Control Element with Excessive Volume of Commented-out Code	1400	1925
HasMember	B	1086	Class with Excessive Number of Child Classes	1400	1926
HasMember	B	1087	Class with Virtual Method without a Virtual Destructor	1400	1927
HasMember	B	1090	Method Containing Access of a Member Element from Another Class	1400	1930
HasMember	B	1092	Use of Same Invokable Control Element in Multiple Architectural Layers	1400	1932
HasMember	C	1093	Excessively Complex Data Representation	1400	1933
HasMember	B	1095	Loop Condition Value Update within the Loop	1400	1935
HasMember	B	1097	Persistent Storable Data Element without Associated Comparison Control Element	1400	1937
HasMember	B	1098	Data Element containing Pointer Item without Proper Copy Control Element	1400	1938
HasMember	B	1099	Inconsistent Naming Conventions for Identifiers	1400	1939
HasMember	B	1100	Insufficient Isolation of System-Dependent Functions	1400	1940
HasMember	B	1101	Reliance on Runtime Component in Generated Code	1400	1941
HasMember	B	1102	Reliance on Machine-Dependent Data Representation	1400	1942
HasMember	B	1103	Use of Platform-Dependent Third Party Components	1400	1943
HasMember	B	1105	Insufficient Encapsulation of Machine-Dependent Functionality	1400	1945
HasMember	B	1106	Insufficient Use of Symbolic Constants	1400	1946
HasMember	B	1107	Insufficient Isolation of Symbolic Constant Definitions	1400	1947
HasMember	B	1108	Excessive Reliance on Global Variables	1400	1948
HasMember	B	1109	Use of Same Variable for Multiple Purposes	1400	1949
HasMember	B	1110	Incomplete Design Documentation	1400	1950
HasMember	B	1111	Incomplete I/O Documentation	1400	1951
HasMember	B	1112	Incomplete Documentation of Program Execution	1400	1952
HasMember	B	1113	Inappropriate Comment Style	1400	1953
HasMember	B	1114	Inappropriate Whitespace Style	1400	1953

Nature	Type	ID	Name	V	Page
HasMember	B	1115	Source Code Element without Standard Prologue	1400	1954
HasMember	B	1116	Inaccurate Comments	1400	1955
HasMember	B	1117	Callable with Insufficient Behavioral Summary	1400	1957
HasMember	B	1118	Insufficient Documentation of Error Handling Techniques	1400	1958
HasMember	B	1119	Excessive Use of Unconditional Branching	1400	1959
HasMember	C	1120	Excessive Code Complexity	1400	1960
HasMember	B	1121	Excessive McCabe Cyclomatic Complexity	1400	1961
HasMember	B	1122	Excessive Halstead Complexity	1400	1962
HasMember	B	1123	Excessive Use of Self-Modifying Code	1400	1963
HasMember	B	1124	Excessively Deep Nesting	1400	1964
HasMember	B	1125	Excessive Attack Surface	1400	1965
HasMember	B	1126	Declaration of Variable with Unnecessarily Wide Scope	1400	1966
HasMember	B	1127	Compilation with Insufficient Warnings or Errors	1400	1966
HasMember	C	1164	Irrelevant Code	1400	1967
HasMember	C	1177	Use of Prohibited Code	1400	1972
HasMember	B	1209	Failure to Disable Reserved Bits	1400	1991
HasMember	B	1245	Improper Finite State Machines (FSMs) in Hardware Logic	1400	2041
HasMember	B	1341	Multiple Releases of Same Resource or Handle	1400	2246
HasMember	C	1357	Reliance on Insufficiently Trustworthy Component	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 >.

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	2598
HasMember	B	182	Collapse of Data into Unsafe Value	1400	455
HasMember	B	184	Incomplete List of Disallowed Inputs	1400	459
HasMember	B	222	Truncation of Security-relevant Information	1400	557
HasMember	B	223	Omission of Security-relevant Information	1400	559
HasMember	B	224	Obscured Security-relevant Information by Alternate Name	1400	561
HasMember	B	356	Product UI does not Warn User of Unsafe Actions	1400	879
HasMember	B	357	Insufficient UI Warning of Dangerous Operations	1400	880
HasMember	B	450	Multiple Interpretations of UI Input	1400	1078
HasMember	C	602	Client-Side Enforcement of Server-Side Security	1400	1350
HasMember	P	693	Protection Mechanism Failure	1400	1520

Nature	Type	ID	Name	V	Page
HasMember	B	757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')	1400	1581
HasMember	B	778	Insufficient Logging	1400	1638
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1400	1714
HasMember	C	1039	Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations	1400	1873
HasMember	B	1248	Semiconductor Defects in Hardware Logic with Security-Sensitive Implications	1400	2049
HasMember	B	1253	Incorrect Selection of Fuse Values	1400	2058
HasMember	B	1269	Product Released in Non-Release Configuration	1400	2098
HasMember	B	1278	Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques	1400	2118
HasMember	B	1291	Public Key Re-Use for Signing both Debug and Production Code	1400	2145
HasMember	B	1318	Missing Support for Security Features in On-chip Fabrics or Buses	1400	2197
HasMember	B	1319	Improper Protection against Electromagnetic Fault Injection (EM-FI)	1400	2199
HasMember	B	1326	Missing Immutable Root of Trust in Hardware	1400	2212
HasMember	B	1338	Improper Protections Against Hardware Overheating	1400	2240

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	V	6	J2EE Misconfiguration: Insufficient Session-ID Length	1400	2
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	1400	790
HasMember	V	329	Generation of Predictable IV with CBC Mode	1400	811
HasMember	C	330	Use of Insufficiently Random Values	1400	814
HasMember	B	331	Insufficient Entropy	1400	821
HasMember	V	332	Insufficient Entropy in PRNG	1400	823
HasMember	V	333	Improper Handling of Insufficient Entropy in TRNG	1400	825
HasMember	B	334	Small Space of Random Values	1400	827
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	1400	829
HasMember	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)	1400	832

Nature	Type	ID	Name	V	Page
HasMember	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)	1400	834
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	1400	837
HasMember	V	339	Small Seed Space in PRNG	1400	840
HasMember	C	340	Generation of Predictable Numbers or Identifiers	1400	842
HasMember	B	341	Predictable from Observable State	1400	843
HasMember	B	342	Predictable Exact Value from Previous Values	1400	845
HasMember	B	343	Predictable Value Range from Previous Values	1400	847
HasMember	B	344	Use of Invariant Value in Dynamically Changing Context	1400	849
HasMember	B	1204	Generation of Weak Initialization Vector (IV)	1400	1987
HasMember	B	1241	Use of Predictable Algorithm in Random Number Generator	1400	2030

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	B	385	Covert Timing Channel	1400	940
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1400	1118
HasMember	V	473	PHP External Variable Modification	1400	1127
HasMember	B	502	Deserialization of Untrusted Data	1400	1204
HasMember	C	514	Covert Channel	1400	1218
HasMember	B	515	Covert Storage Channel	1400	1220
HasMember	C	672	Operation on a Resource after Expiration or Release	1400	1479
HasMember	B	826	Premature Release of Resource During Expected Lifetime	1400	1734
HasMember	B	910	Use of Expired File Descriptor	1400	1800
HasMember	B	915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	1400	1809
HasMember	B	1104	Use of Unmaintained Third Party Components	1400	1944
HasMember	B	1249	Application-Level Admin Tool with Inconsistent View of Underlying Operating System	1400	2050
HasMember	B	1251	Mirrored Regions with Different Values	1400	2054
HasMember	B	1277	Firmware Not Updateable	1400	2116
HasMember	B	1310	Missing Ability to Patch ROM Code	1400	2179
HasMember	V	1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	1400	2204

Nature	Type	ID	Name	V	Page
HasMember	B	1329	Reliance on Component That is Not Updateable	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 >.

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	2598
HasMember	V	98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	1400	236
HasMember	C	118	Incorrect Access of Indexable Resource ('Range Error')	1400	292
HasMember	B	178	Improper Handling of Case Sensitivity	1400	445
HasMember	V	192	Integer Coercion Error	1400	482
HasMember	V	194	Unexpected Sign Extension	1400	491
HasMember	V	195	Signed to Unsigned Conversion Error	1400	494
HasMember	V	196	Unsigned to Signed Conversion Error	1400	498
HasMember	B	197	Numeric Truncation Error	1400	500
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	1400	544
HasMember	C	221	Information Loss or Omission	1400	556
HasMember	B	226	Sensitive Information in Resource Not Removed Before Reuse	1400	562
HasMember	V	243	Creation of chroot Jail Without Changing Working Directory	1400	589
HasMember	B	372	Incomplete Internal State Distinction	1400	919
HasMember	B	386	Symbolic Name not Mapping to Correct Object	1400	942
HasMember	C	400	Uncontrolled Resource Consumption	1400	964
HasMember	C	404	Improper Resource Shutdown or Release	1400	980
HasMember	C	405	Asymmetric Resource Consumption (Amplification)	1400	986
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	1400	990
HasMember	C	407	Inefficient Algorithmic Complexity	1400	992
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	1400	996
HasMember	B	410	Insufficient Resource Pool	1400	998
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1400	1048
HasMember	V	453	Insecure Default Variable Initialization	1400	1083
HasMember	B	454	External Initialization of Trusted Variables or Data Stores	1400	1085

Nature	Type	ID	Name	V	Page
HasMember	V	456	Missing Initialization of a Variable	1400	1089
HasMember	V	457	Use of Uninitialized Variable	1400	1094
HasMember	B	459	Incomplete Cleanup	1400	1099
HasMember	B	460	Improper Cleanup on Thrown Exception	1400	1102
HasMember	B	471	Modification of Assumed-Immutable Data (MAID)	1400	1121
HasMember	B	487	Reliance on Package-level Scope	1400	1167
HasMember	V	495	Private Data Structure Returned From A Public Method	1400	1189
HasMember	V	496	Public Data Assigned to Private Array-Typed Field	1400	1192
HasMember	B	501	Trust Boundary Violation	1400	1203
HasMember	V	568	finalize() Method Without super.finalize()	1400	1290
HasMember	V	580	clone() Method Without super.clone()	1400	1311
HasMember	V	588	Attempt to Access Child of a Non-structure Pointer	1400	1323
HasMember	V	607	Public Static Final Field References Mutable Object	1400	1360
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1400	1364
HasMember	V	618	Exposed Unsafe ActiveX Method	1400	1380
HasMember	C	662	Improper Synchronization	1400	1448
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1400	1454
HasMember	C	665	Improper Initialization	1400	1456
HasMember	C	666	Operation on Resource in Wrong Phase of Lifetime	1400	1462
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1400	1471
HasMember	C	673	External Influence of Sphere Definition	1400	1483
HasMember	B	681	Incorrect Conversion between Numeric Types	1400	1495
HasMember	C	704	Incorrect Type Conversion or Cast	1400	1538
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	1400	1544
HasMember	B	749	Exposed Dangerous Method or Function	1400	1564
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1400	1613
HasMember	B	771	Missing Reference to Active Allocated Resource	1400	1622
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1400	1624
HasMember	V	773	Missing Reference to Active File Descriptor or Handle	1400	1629
HasMember	V	774	Allocation of File Descriptors or Handles Without Limits or Throttling	1400	1630
HasMember	V	775	Missing Release of File Descriptor or Handle after Effective Lifetime	1400	1631
HasMember	B	776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	1400	1633
HasMember	B	779	Logging of Excessive Data	1400	1642
HasMember	V	782	Exposed IOCTL with Insufficient Access Control	1400	1648
HasMember	V	827	Improper Control of Document Type Definition	1400	1736
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1400	1741
HasMember	V	830	Inclusion of Web Functionality from an Untrusted Source	1400	1747
HasMember	B	843	Access of Resource Using Incompatible Type ('Type Confusion')	1400	1776
HasMember	B	908	Use of Uninitialized Resource	1400	1792
HasMember	C	909	Missing Initialization of Resource	1400	1797
HasMember	B	911	Improper Update of Reference Count	1400	1801
HasMember	C	913	Improper Control of Dynamically-Managed Code Resources	1400	1805
HasMember	B	920	Improper Restriction of Power Consumption	1400	1823

Nature	Type	ID	Name	V	Page
HasMember	C	922	Insecure Storage of Sensitive Information	1400	1825
HasMember	V	1042	Static Member Data Element outside of a Singleton Class Element	1400	1876
HasMember	B	1046	Creation of Immutable Text Using String Concatenation	1400	1881
HasMember	B	1049	Excessive Data Query Operations in a Large Data Table	1400	1884
HasMember	B	1050	Excessive Platform Resource Consumption within a Loop	1400	1885
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1400	1886
HasMember	B	1052	Excessive Use of Hard-Coded Literals in Initialization	1400	1887
HasMember	B	1063	Creation of Class Instance within a Static Code Block	1400	1901
HasMember	B	1067	Excessive Execution of Sequential Searches of Data Resource	1400	1905
HasMember	B	1072	Data Resource Access without Use of Connection Pooling	1400	1912
HasMember	B	1073	Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses	1400	1913
HasMember	B	1084	Invokable Control Element with Excessive File or Data Access Operations	1400	1924
HasMember	B	1089	Large Data Table with Excessive Number of Indices	1400	1929
HasMember	B	1091	Use of Object without Invoking Destructor Method	1400	1931
HasMember	B	1094	Excessive Index Range Scan for a Data Resource	1400	1934
HasMember	C	1176	Inefficient CPU Computation	1400	1971
HasMember	B	1188	Initialization of a Resource with an Insecure Default	1400	1974
HasMember	B	1221	Incorrect Register Defaults or Module Parameters	1400	1996
HasMember	C	1229	Creation of Emergent Resource	1400	2006
HasMember	B	1235	Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations	1400	2017
HasMember	V	1239	Improper Zeroization of Hardware Register	1400	2022
HasMember	B	1246	Improper Write Handling in Limited-write Non-Volatile Memories	1400	2043
HasMember	B	1250	Improper Preservation of Consistency Between Independent Representations of Shared State	1400	2052
HasMember	B	1258	Exposure of Sensitive System Information Due to Uncleared Debug Information	1400	2071
HasMember	B	1266	Improper Scrubbing of Sensitive Data from Decommissioned Device	1400	2091
HasMember	B	1271	Uninitialized Value on Reset for Registers Holding Security Settings	1400	2102
HasMember	B	1272	Sensitive Information Uncleared Before Debug/Power State Transition	1400	2104
HasMember	B	1279	Cryptographic Operations are run Before Supporting Units are Ready	1400	2120
HasMember	B	1301	Insufficient or Incomplete Data Removal within Hardware Component	1400	2170
HasMember	B	1325	Improperly Controlled Sequential Memory Allocation	1400	2210
HasMember	V	1330	Remanent Data Readable after Memory Erase	1400	2222
HasMember	B	1333	Inefficient Regular Expression Complexity	1400	2230
HasMember	B	1342	Information Exposure through Microarchitectural State after Transient Execution	1400	2250

Nature	Type	ID	Name	V	Page
HasMember	B	1386	Insecure Operation on Windows Junction / Mount Point	1400	2261
HasMember	B	1389	Incorrect Parsing of Numbers with Different Radices	1400	2263
HasMember	C	1419	Incorrect Initialization of Resource	1400	2280
HasMember	B	1420	Exposure of Sensitive Information during Transient Execution	1400	2284
HasMember	B	1421	Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution	1400	2290
HasMember	B	1422	Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution	1400	2297
HasMember	B	1423	Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution	1400	2302

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	1400	504
HasMember	B	201	Insertion of Sensitive Information Into Sent Data	1400	514
HasMember	B	203	Observable Discrepancy	1400	518
HasMember	B	204	Observable Response Discrepancy	1400	523
HasMember	B	205	Observable Behavioral Discrepancy	1400	526
HasMember	V	206	Observable Internal Behavioral Discrepancy	1400	527
HasMember	V	207	Observable Behavioral Discrepancy With Equivalent Products	1400	528
HasMember	B	208	Observable Timing Discrepancy	1400	529
HasMember	B	209	Generation of Error Message Containing Sensitive Information	1400	533
HasMember	B	210	Self-generated Error Message Containing Sensitive Information	1400	539
HasMember	B	211	Externally-Generated Error Message Containing Sensitive Information	1400	541
HasMember	B	213	Exposure of Sensitive Information Due to Incompatible Policies	1400	547
HasMember	B	214	Invocation of Process Using Visible Sensitive Information	1400	549
HasMember	B	215	Insertion of Sensitive Information Into Debugging Code	1400	551

Nature	Type	ID	Name	V	Page
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	1400	882
HasMember	B	497	Exposure of Sensitive System Information to an Unauthorized Control Sphere	1400	1193
HasMember	V	526	Cleartext Storage of Sensitive Information in an Environment Variable	1400	1234
HasMember	V	531	Inclusion of Sensitive Information in Test Code	1400	1240
HasMember	B	532	Insertion of Sensitive Information into Log File	1400	1241
HasMember	V	535	Exposure of Information Through Shell Error Message	1400	1244
HasMember	V	536	Servlet Runtime Error Message Containing Sensitive Information	1400	1245
HasMember	V	537	Java Runtime Error Message Containing Sensitive Information	1400	1246
HasMember	B	538	Insertion of Sensitive Information into Externally-Accessible File or Directory	1400	1248
HasMember	B	540	Inclusion of Sensitive Information in Source Code	1400	1251
HasMember	V	541	Inclusion of Sensitive Information in an Include File	1400	1253
HasMember	V	548	Exposure of Information Through Directory Listing	1400	1261
HasMember	V	550	Server-generated Error Message Containing Sensitive Information	1400	1263
HasMember	V	598	Use of GET Request Method With Sensitive Query Strings	1400	1340
HasMember	V	615	Inclusion of Sensitive Information in Source Code Comments	1400	1375
HasMember	V	651	Exposure of WSDL File Containing Sensitive Information	1400	1433
HasMember	B	1254	Incorrect Comparison Logic Granularity	1400	2060
HasMember	V	1255	Comparison Logic is Vulnerable to Power Side-Channel Attacks	1400	2062
HasMember	B	1273	Device Unlock Credential Sharing	1400	2106
HasMember	B	1295	Debug Messages Revealing Unnecessary Information	1400	2152
HasMember	B	1300	Improper Protection of Physical Side Channels	1400	2165

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2598
HasMember	B	250	Execution with Unnecessary Privileges	1400	599

Nature	Type	ID	Name	V	Page
HasMember	C	424	Improper Protection of Alternate Path	1400	1023
HasMember	B	447	Unimplemented or Unsupported Feature in UI	1400	1075
HasMember	C	636	Not Failing Securely ('Failing Open')	1400	1401
HasMember	C	637	Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism')	1400	1403
HasMember	C	638	Not Using Complete Mediation	1400	1404
HasMember	C	653	Improper Isolation or Compartmentalization	1400	1437
HasMember	B	654	Reliance on a Single Factor in a Security Decision	1400	1439
HasMember	C	655	Insufficient Psychological Acceptability	1400	1442
HasMember	C	656	Reliance on Security Through Obscurity	1400	1444
HasMember	C	657	Violation of Secure Design Principles	1400	1446
HasMember	C	671	Lack of Administrator Control over Security	1400	1478
HasMember	B	1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)	1400	1976
HasMember	B	1192	Improper Identifier for IP Block used in System-On-Chip (SOC)	1400	1985
HasMember	B	1303	Non-Transparent Sharing of Microarchitectural Resources	1400	2174
HasMember	B	1331	Improper Isolation of Shared Resources in Network On Chip (NoC)	1400	2225
HasMember	C	1395	Dependency on Vulnerable Third-Party Component	1400	2277

References

[REF-1330]MITRE. "CVE --> CWE Mapping Guidance - Quick Tips". 2021 March 5. < https://cwe.mitre.org/documents/cwe_usage/quick_tips.html >.

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	2550

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)	2330
HasMember	C	713	OWASP Top Ten 2007 Category A2 - Injection Flaws	2330
HasMember	C	714	OWASP Top Ten 2007 Category A3 - Malicious File Execution	2331
HasMember	C	715	OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference	2331
HasMember	C	716	OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF)	2331
HasMember	C	717	OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling	2332
HasMember	C	718	OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management	2332
HasMember	C	719	OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage	2333
HasMember	C	720	OWASP Top Ten 2007 Category A9 - Insecure Communications	2333
HasMember	C	721	OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access	2333

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	938
Categories	10	out of	374
Views	0	out of	50
Total	38	out of	1362

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	2309
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')	111
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	219
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	B	134	Use of Externally-Controlled Format String	365
HasMember	C	189	Numeric Errors	2312
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	504
HasMember	C	255	Credentials Management Errors	2315
HasMember	C	264	Permissions, Privileges, and Access Controls	2316
HasMember	C	287	Improper Authentication	692
HasMember	C	310	Cryptographic Issues	2318
HasMember		352	Cross-Site Request Forgery (CSRF)	868
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	888
HasMember	C	399	Resource Management Errors	2324

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	938
Categories	6	out of	374
Views	0	out of	50
Total	19	out of	1362

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	2553

Metrics

	CWEs in this view		Total CWEs
Weaknesses	82	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	82	out of	1362

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++	2553

Metrics

	CWEs in this view		Total CWEs
Weaknesses	86	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	86	out of	1362

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	2554

Metrics

	CWEs in this view		Total CWEs
Weaknesses	77	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	77	out of	1362

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	2554

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	25	out of	1362

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	2554

Metrics

	CWEs in this view		Total CWEs
Weaknesses	519	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	519	out of	1362

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	2555

Metrics

	CWEs in this view		Total CWEs
Weaknesses	4	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	4	out of	1362

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	2309
HasMember	C	133	String Errors	2310
HasMember	C	136	Type Errors	2310
HasMember	C	137	Data Neutralization Issues	2311
HasMember	C	189	Numeric Errors	2312
HasMember	C	199	Information Management Errors	2312
HasMember	C	255	Credentials Management Errors	2315
HasMember	C	265	Privilege Issues	2316
HasMember	C	275	Permission Issues	2317
HasMember	C	310	Cryptographic Issues	2318
HasMember	C	320	Key Management Errors	2319
HasMember	C	355	User Interface Security Issues	2320
HasMember	C	371	State Issues	2321
HasMember	C	387	Signal Errors	2321
HasMember	C	389	Error Conditions, Return Values, Status Codes	2322
HasMember	C	399	Resource Management Errors	2324
HasMember	C	411	Resource Locking Problems	2325
HasMember	C	417	Communication Channel Errors	2325
HasMember	C	429	Handler Errors	2326
HasMember	C	438	Behavioral Problems	2326
HasMember	C	452	Initialization and Cleanup Errors	2327
HasMember	C	465	Pointer Issues	2328
HasMember	C	557	Concurrency Issues	2329
HasMember	C	569	Expression Issues	2330
HasMember	C	840	Business Logic Errors	2360
HasMember	C	1006	Bad Coding Practices	2422
HasMember	C	1210	Audit / Logging Errors	2475
HasMember	C	1211	Authentication Errors	2475
HasMember	C	1212	Authorization Errors	2476
HasMember	C	1213	Random Number Issues	2477
HasMember	C	1214	Data Integrity Issues	2477
HasMember	C	1215	Data Validation Issues	2478
HasMember	C	1216	Lockout Mechanism Errors	2478
HasMember	C	1217	User Session Errors	2479
HasMember	C	1218	Memory Buffer Errors	2479
HasMember	C	1219	File Handling Issues	2480
HasMember	C	1225	Documentation Issues	2480
HasMember	C	1226	Complexity Issues	2481
HasMember	C	1227	Encapsulation Issues	2481
HasMember	C	1228	API / Function Errors	2482

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	938
Categories	40	out of	374
Views	0	out of	50
Total	439	out of	1362

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	2308
HasMember	C	227	7PK - API Abuse	2313
HasMember	C	254	7PK - Security Features	2314
HasMember	C	361	7PK - Time and State	2320
HasMember	C	388	7PK - Errors	2322
HasMember	C	398	7PK - Code Quality	2323
HasMember	C	485	7PK - Encapsulation	2328
HasMember	C	1005	7PK - Input Validation and Representation	2421

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	938
Categories	9	out of	374
Views	0	out of	50
Total	97	out of	1362

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	2558

Metrics

	CWEs in this view		Total CWEs
Weaknesses	272	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	272	out of	1362

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	2558

Metrics

	CWEs in this view		Total CWEs
Weaknesses	732	out of	938
Categories	0	out of	374
Views	0	out of	50

	CWEs in this view		Total CWEs
Total	732	out of	1362

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	2559

Metrics

	CWEs in this view		Total CWEs
Weaknesses	3	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	3	out of	1362

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	2334

Nature	Type	ID	Name	Page
HasMember	C	723	OWASP Top Ten 2004 Category A2 - Broken Access Control	2335
HasMember	C	724	OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management	2335
HasMember	C	725	OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws	2336
HasMember	C	726	OWASP Top Ten 2004 Category A5 - Buffer Overflows	2336
HasMember	C	727	OWASP Top Ten 2004 Category A6 - Injection Flaws	2337
HasMember	C	728	OWASP Top Ten 2004 Category A7 - Improper Error Handling	2337
HasMember	C	729	OWASP Top Ten 2004 Category A8 - Insecure Storage	2338
HasMember	C	730	OWASP Top Ten 2004 Category A9 - Denial of Service	2339
HasMember	C	731	OWASP Top Ten 2004 Category A10 - Insecure Configuration Management	2339

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	938
Categories	13	out of	374
Views	0	out of	50
Total	130	out of	1362

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)	2340
HasMember	C	736	CERT C Secure Coding Standard (2008) Chapter 3 - Declarations and Initialization (DCL)	2341
HasMember	C	737	CERT C Secure Coding Standard (2008) Chapter 4 - Expressions (EXP)	2341
HasMember	C	738	CERT C Secure Coding Standard (2008) Chapter 5 - Integers (INT)	2342
HasMember	C	739	CERT C Secure Coding Standard (2008) Chapter 6 - Floating Point (FLP)	2343
HasMember	C	740	CERT C Secure Coding Standard (2008) Chapter 7 - Arrays (ARR)	2344
HasMember	C	741	CERT C Secure Coding Standard (2008) Chapter 8 - Characters and Strings (STR)	2344
HasMember	C	742	CERT C Secure Coding Standard (2008) Chapter 9 - Memory Management (MEM)	2345
HasMember	C	743	CERT C Secure Coding Standard (2008) Chapter 10 - Input Output (FIO)	2347
HasMember	C	744	CERT C Secure Coding Standard (2008) Chapter 11 - Environment (ENV)	2348
HasMember	C	745	CERT C Secure Coding Standard (2008) Chapter 12 - Signals (SIG)	2349
HasMember	C	746	CERT C Secure Coding Standard (2008) Chapter 13 - Error Handling (ERR)	2350
HasMember	C	747	CERT C Secure Coding Standard (2008) Chapter 14 - Miscellaneous (MSC)	2350
HasMember	C	748	CERT C Secure Coding Standard (2008) Appendix - POSIX (POS)	2351

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	938
Categories	14	out of	374
Views	0	out of	50
Total	105	out of	1362

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	2352
HasMember	C	752	2009 Top 25 - Risky Resource Management	2353
HasMember	C	753	2009 Top 25 - Porous Defenses	2353

References

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

Metrics

	CWEs in this view		Total CWEs
Weaknesses	26	out of	938
Categories	3	out of	374
Views	0	out of	50
Total	29	out of	1362

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	2354
HasMember	C	802	2010 Top 25 - Risky Resource Management	2354
HasMember	C	803	2010 Top 25 - Porous Defenses	2355
HasMember	C	808	2010 Top 25 - Weaknesses On the Cusp	2355

References

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

Metrics

	CWEs in this view		Total CWEs
Weaknesses	41	out of	938
Categories	4	out of	374
Views	0	out of	50
Total	45	out of	1362

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	2356
HasMember	C	811	OWASP Top Ten 2010 Category A2 - Cross-Site Scripting (XSS)	2357
HasMember	C	812	OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management	2357
HasMember	C	813	OWASP Top Ten 2010 Category A4 - Insecure Direct Object References	2357
HasMember	C	814	OWASP Top Ten 2010 Category A5 - Cross-Site Request Forgery(CSRF)	2358
HasMember	C	815	OWASP Top Ten 2010 Category A6 - Security Misconfiguration	2358
HasMember	C	816	OWASP Top Ten 2010 Category A7 - Insecure Cryptographic Storage	2359
HasMember	C	817	OWASP Top Ten 2010 Category A8 - Failure to Restrict URL Access	2359
HasMember	C	818	OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection	2359
HasMember	C	819	OWASP Top Ten 2010 Category A10 - Unvalidated Redirects and Forwards	2360

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	938
Categories	10	out of	374
Views	0	out of	50
Total	42	out of	1362

View-844: Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011)

View ID : 844
Type : Graph

Objective

2564

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)	2362
HasMember	C	846	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 3 - Declarations and Initialization (DCL)	2362
HasMember	C	847	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 4 - Expressions (EXP)	2363
HasMember	C	848	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 5 - Numeric Types and Operations (NUM)	2363
HasMember	C	849	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 6 - Object Orientation (OBJ)	2364
HasMember	C	850	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 7 - Methods (MET)	2364
HasMember	C	851	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 8 - Exceptional Behavior (ERR)	2365
HasMember	C	852	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 9 - Visibility and Atomicity (VNA)	2366
HasMember	C	853	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 10 - Locking (LCK)	2366
HasMember	C	854	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 11 - Thread APIs (THI)	2367
HasMember	C	855	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 12 - Thread Pools (TPS)	2367
HasMember	C	856	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 13 - Thread-Safety Miscellaneous (TSM)	2367
HasMember	C	857	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 14 - Input Output (FIO)	2368
HasMember	C	858	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 15 - Serialization (SER)	2368
HasMember	C	859	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 16 - Platform Security (SEC)	2369
HasMember	C	860	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 17 - Runtime Environment (ENV)	2370

Nature	Type	ID	Name	Page
HasMember	C	861	The CERT Oracle Secure Coding Standard for Java (2011) Chapter 18 - Miscellaneous (MSC)	2370

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	938
Categories	17	out of	374
Views	0	out of	50
Total	121	out of	1362

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)	2373

Nature	Type	ID	Name	Page
HasMember	C	870	CERT C++ Secure Coding Section 02 - Declarations and Initialization (DCL)	2373
HasMember	C	871	CERT C++ Secure Coding Section 03 - Expressions (EXP)	2374
HasMember	C	872	CERT C++ Secure Coding Section 04 - Integers (INT)	2374
HasMember	C	873	CERT C++ Secure Coding Section 05 - Floating Point Arithmetic (FLP)	2375
HasMember	C	874	CERT C++ Secure Coding Section 06 - Arrays and the STL (ARR)	2375
HasMember	C	875	CERT C++ Secure Coding Section 07 - Characters and Strings (STR)	2376
HasMember	C	876	CERT C++ Secure Coding Section 08 - Memory Management (MEM)	2376
HasMember	C	877	CERT C++ Secure Coding Section 09 - Input Output (FIO)	2377
HasMember	C	878	CERT C++ Secure Coding Section 10 - Environment (ENV)	2378
HasMember	C	879	CERT C++ Secure Coding Section 11 - Signals (SIG)	2379
HasMember	C	880	CERT C++ Secure Coding Section 12 - Exceptions and Error Handling (ERR)	2379
HasMember	C	881	CERT C++ Secure Coding Section 13 - Object Oriented Programming (OOP)	2380
HasMember	C	882	CERT C++ Secure Coding Section 14 - Concurrency (CON)	2380
HasMember	C	883	CERT C++ Secure Coding Section 49 - Miscellaneous (MSC)	2381

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	938
Categories	15	out of	374
Views	0	out of	50
Total	110	out of	1362

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	86
HasMember	B	59	Improper Link Resolution Before File Access ('Link Following')	111
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	194
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	212
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	219
HasMember	V	95	Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')	226
HasMember	B	96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')	232
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	243
HasMember	V	113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')	271
HasMember	B	117	Improper Output Neutralization for Logs	288
HasMember	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	304
HasMember	V	129	Improper Validation of Array Index	341
HasMember	B	131	Incorrect Calculation of Buffer Size	355
HasMember	B	134	Use of Externally-Controlled Format String	365
HasMember	B	135	Incorrect Calculation of Multi-Byte String Length	370
HasMember	B	170	Improper Null Termination	428
HasMember	V	173	Improper Handling of Alternate Encoding	435
HasMember	V	174	Double Decoding of the Same Data	437
HasMember	V	175	Improper Handling of Mixed Encoding	439
HasMember	B	179	Incorrect Behavior Order: Early Validation	448
HasMember	C	185	Incorrect Regular Expression	463
HasMember	B	190	Integer Overflow or Wraparound	472
HasMember	B	191	Integer Underflow (Wrap or Wraparound)	480
HasMember	B	193	Off-by-one Error	486
HasMember	B	203	Observable Discrepancy	518
HasMember	B	209	Generation of Error Message Containing Sensitive Information	533
HasMember	B	212	Improper Removal of Sensitive Information Before Storage or Transfer	544
HasMember	B	222	Truncation of Security-relevant Information	557
HasMember	B	223	Omission of Security-relevant Information	559
HasMember	C	228	Improper Handling of Syntactically Invalid Structure	568

Nature	Type	ID	Name	Page
HasMember	V	244	Improper Clearing of Heap Memory Before Release ('Heap Inspection')	591
HasMember	B	248	Uncaught Exception	596
HasMember	B	250	Execution with Unnecessary Privileges	599
HasMember	B	252	Unchecked Return Value	606
HasMember	B	253	Incorrect Check of Function Return Value	613
HasMember	B	262	Not Using Password Aging	633
HasMember	B	263	Password Aging with Long Expiration	636
HasMember	B	266	Incorrect Privilege Assignment	638
HasMember	B	267	Privilege Defined With Unsafe Actions	641
HasMember	B	268	Privilege Chaining	644
HasMember	B	270	Privilege Context Switching Error	651
HasMember	C	271	Privilege Dropping / Lowering Errors	653
HasMember	B	273	Improper Check for Dropped Privileges	660
HasMember	B	283	Unverified Ownership	678
HasMember	B	290	Authentication Bypass by Spoofing	705
HasMember	B	294	Authentication Bypass by Capture-replay	712
HasMember	B	296	Improper Following of a Certificate's Chain of Trust	719
HasMember	B	299	Improper Check for Certificate Revocation	727
HasMember	C	300	Channel Accessible by Non-Endpoint	730
HasMember	B	301	Reflection Attack in an Authentication Protocol	733
HasMember	B	304	Missing Critical Step in Authentication	738
HasMember	B	306	Missing Authentication for Critical Function	741
HasMember	B	307	Improper Restriction of Excessive Authentication Attempts	747
HasMember	B	308	Use of Single-factor Authentication	752
HasMember	B	312	Cleartext Storage of Sensitive Information	764
HasMember	B	319	Cleartext Transmission of Sensitive Information	779
HasMember	B	322	Key Exchange without Entity Authentication	788
HasMember	B	323	Reusing a Nonce, Key Pair in Encryption	790
HasMember	B	325	Missing Cryptographic Step	794
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	799
HasMember	B	331	Insufficient Entropy	821
HasMember	B	334	Small Space of Random Values	827
HasMember	B	335	Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)	829
HasMember	B	338	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	837
HasMember	B	341	Predictable from Observable State	843
HasMember	B	347	Improper Verification of Cryptographic Signature	857
HasMember	B	348	Use of Less Trusted Source	859
HasMember	B	349	Acceptance of Extraneous Untrusted Data With Trusted Data	861
HasMember	♣	352	Cross-Site Request Forgery (CSRF)	868
HasMember	B	353	Missing Support for Integrity Check	874
HasMember	B	354	Improper Validation of Integrity Check Value	876
HasMember	B	364	Signal Handler Race Condition	899
HasMember	B	367	Time-of-check Time-of-use (TOCTOU) Race Condition	906
HasMember	B	369	Divide By Zero	913
HasMember	B	390	Detection of Error Condition Without Action	943

Nature	Type	ID	Name	Page
HasMember	B	392	Missing Report of Error Condition	951
HasMember	B	393	Return of Wrong Status Code	953
HasMember	C	400	Uncontrolled Resource Consumption	964
HasMember	C	406	Insufficient Control of Network Message Volume (Network Amplification)	990
HasMember	C	407	Inefficient Algorithmic Complexity	992
HasMember	B	408	Incorrect Behavior Order: Early Amplification	995
HasMember	B	409	Improper Handling of Highly Compressed Data (Data Amplification)	996
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')	1068
HasMember	C	451	User Interface (UI) Misrepresentation of Critical Information	1079
HasMember	V	453	Insecure Default Variable Initialization	1083
HasMember	B	454	External Initialization of Trusted Variables or Data Stores	1085
HasMember	B	455	Non-exit on Failed Initialization	1087
HasMember	V	456	Missing Initialization of a Variable	1089
HasMember	V	467	Use of sizeof() on a Pointer Type	1110
HasMember	B	468	Incorrect Pointer Scaling	1114
HasMember	B	469	Use of Pointer Subtraction to Determine Size	1115
HasMember	B	470	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')	1118
HasMember	B	476	NULL Pointer Dereference	1132
HasMember	B	478	Missing Default Case in Multiple Condition Expression	1142
HasMember	B	480	Use of Incorrect Operator	1150
HasMember	B	483	Incorrect Block Delimitation	1160
HasMember	B	484	Omitted Break Statement in Switch	1162
HasMember	V	486	Comparison of Classes by Name	1164
HasMember	B	494	Download of Code Without Integrity Check	1185
HasMember	V	495	Private Data Structure Returned From A Public Method	1189
HasMember	V	496	Public Data Assigned to Private Array-Typed Field	1192
HasMember	V	498	Cloneable Class Containing Sensitive Information	1196
HasMember	V	499	Serializable Class Containing Sensitive Data	1198
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	B	521	Weak Password Requirements	1223
HasMember	C	522	Insufficiently Protected Credentials	1225
HasMember	V	546	Suspicious Comment	1258
HasMember	B	547	Use of Hard-coded, Security-relevant Constants	1259
HasMember	B	561	Dead Code	1275
HasMember	B	563	Assignment to Variable without Use	1280
HasMember	B	567	Unsynchronized Access to Shared Data in a Multithreaded Context	1288
HasMember	V	587	Assignment of a Fixed Address to a Pointer	1322
HasMember	V	595	Comparison of Object References Instead of Object Contents	1334
HasMember	B	601	URL Redirection to Untrusted Site ('Open Redirect')	1345
HasMember	C	602	Client-Side Enforcement of Server-Side Security	1350
HasMember	V	605	Multiple Binds to the Same Port	1356
HasMember	B	617	Reachable Assertion	1378
HasMember	V	621	Variable Extraction Error	1385

Nature	Type	ID	Name	Page
HasMember	V	627	Dynamic Variable Evaluation	1396
HasMember	B	628	Function Call with Incorrectly Specified Arguments	1398
HasMember	C	642	External Control of Critical State Data	1414
HasMember	B	648	Incorrect Use of Privileged APIs	1428
HasMember	C	667	Improper Locking	1464
HasMember	C	672	Operation on a Resource after Expiration or Release	1479
HasMember	C	674	Uncontrolled Recursion	1484
HasMember	B	676	Use of Potentially Dangerous Function	1489
HasMember	B	681	Incorrect Conversion between Numeric Types	1495
HasMember	B	698	Execution After Redirect (EAR)	1533
HasMember	B	708	Incorrect Ownership Assignment	1548
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1551
HasMember	B	756	Missing Custom Error Page	1579
HasMember	B	763	Release of Invalid Pointer or Reference	1599
HasMember	B	770	Allocation of Resources Without Limits or Throttling	1613
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1624
HasMember	B	783	Operator Precedence Logic Error	1650
HasMember	B	786	Access of Memory Location Before Start of Buffer	1658
HasMember	B	788	Access of Memory Location After End of Buffer	1669
HasMember	B	798	Use of Hard-coded Credentials	1690
HasMember	B	805	Buffer Access with Incorrect Length Value	1702
HasMember	B	807	Reliance on Untrusted Inputs in a Security Decision	1714
HasMember	B	822	Untrusted Pointer Dereference	1723
HasMember	B	825	Expired Pointer Dereference	1732
HasMember	B	829	Inclusion of Functionality from Untrusted Control Sphere	1741
HasMember	B	835	Loop with Unreachable Exit Condition ('Infinite Loop')	1757
HasMember	B	838	Inappropriate Encoding for Output Context	1764
HasMember	B	839	Numeric Range Comparison Without Minimum Check	1767
HasMember	B	841	Improper Enforcement of Behavioral Workflow	1772
HasMember	C	862	Missing Authorization	1780
HasMember	C	863	Incorrect Authorization	1787

Metrics

	CWEs in this view		Total CWEs
Weaknesses	157	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	157	out of	1362

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	2382
HasMember	C	886	SFP Primary Cluster: Unused entities	2382
HasMember	C	887	SFP Primary Cluster: API	2382
HasMember	C	889	SFP Primary Cluster: Exception Management	2382
HasMember	C	890	SFP Primary Cluster: Memory Access	2383
HasMember	C	891	SFP Primary Cluster: Memory Management	2383
HasMember	C	892	SFP Primary Cluster: Resource Management	2383
HasMember	C	893	SFP Primary Cluster: Path Resolution	2384
HasMember	C	894	SFP Primary Cluster: Synchronization	2384
HasMember	C	895	SFP Primary Cluster: Information Leak	2384
HasMember	C	896	SFP Primary Cluster: Tainted Input	2385
HasMember	C	897	SFP Primary Cluster: Entry Points	2385
HasMember	C	898	SFP Primary Cluster: Authentication	2385
HasMember	C	899	SFP Primary Cluster: Access Control	2386
HasMember	C	901	SFP Primary Cluster: Privilege	2386
HasMember	C	902	SFP Primary Cluster: Channel	2387
HasMember	C	903	SFP Primary Cluster: Cryptography	2387
HasMember	C	904	SFP Primary Cluster: Malware	2387
HasMember	C	905	SFP Primary Cluster: Predictability	2388
HasMember	C	906	SFP Primary Cluster: UI	2388
HasMember	C	907	SFP Primary Cluster: Other	2388
HasMember	C	1237	SFP Primary Cluster: Faulty Resource Release	2482
HasMember	C	1238	SFP Primary Cluster: Failure to Release Memory	2482

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	938
Categories	83	out of	374
Views	0	out of	50
Total	697	out of	1362

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	2371
HasMember	C	865	2011 Top 25 - Risky Resource Management	2371
HasMember	C	866	2011 Top 25 - Porous Defenses	2372
HasMember	C	867	2011 Top 25 - Weaknesses On the Cusp	2372

References

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

Metrics

	CWEs in this view		Total CWEs
Weaknesses	41	out of	938
Categories	4	out of	374
Views	0	out of	50
Total	45	out of	1362

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	2573

Metrics

	CWEs in this view		Total CWEs
Weaknesses	21	out of	938
Categories	0	out of	374
Views	0	out of	50

	CWEs in this view		Total CWEs
Total	21	out of	1362

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	2389
HasMember	C	930	OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management	2389
HasMember	C	931	OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS)	2390
HasMember	C	932	OWASP Top Ten 2013 Category A4 - Insecure Direct Object References	2390
HasMember	C	933	OWASP Top Ten 2013 Category A5 - Security Misconfiguration	2391
HasMember	C	934	OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure	2391
HasMember	C	935	OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control	2392
HasMember	C	936	OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF)	2392
HasMember	C	937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities	2392
HasMember	C	938	OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards	2393

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	938
Categories	13	out of	374
Views	0	out of	50
Total	49	out of	1362

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	680
HasMember	P	435	Improper Interaction Between Multiple Correctly-Behaving Entities	1055
HasMember	P	664	Improper Control of a Resource Through its Lifetime	1454
HasMember	P	682	Incorrect Calculation	1499
HasMember	P	691	Insufficient Control Flow Management	1517
HasMember	P	693	Protection Mechanism Failure	1520
HasMember	P	697	Incorrect Comparison	1530
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1535
HasMember	P	707	Improper Neutralization	1546
HasMember	P	710	Improper Adherence to Coding Standards	1549

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	938	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	938	out of	1362

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	C	20	Improper Input Validation	20
HasMember	C	74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	137
HasMember	C	116	Improper Encoding or Escaping of Output	281
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	504
HasMember	C	269	Improper Privilege Management	646
HasMember	C	287	Improper Authentication	692
HasMember	C	311	Missing Encryption of Sensitive Data	757
HasMember	C	326	Inadequate Encryption Strength	796
HasMember	C	327	Use of a Broken or Risky Cryptographic Algorithm	799
HasMember	C	330	Use of Insufficiently Random Values	814
HasMember	C	345	Insufficient Verification of Data Authenticity	851
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	888
HasMember	C	400	Uncontrolled Resource Consumption	964
HasMember	C	404	Improper Resource Shutdown or Release	980
HasMember	C	407	Inefficient Algorithmic Complexity	992
HasMember	C	436	Interpretation Conflict	1057

Nature	Type	ID	Name	Page
HasMember	C	610	Externally Controlled Reference to a Resource in Another Sphere	1364
HasMember	C	662	Improper Synchronization	1448
HasMember	C	665	Improper Initialization	1456
HasMember	C	668	Exposure of Resource to Wrong Sphere	1469
HasMember	C	669	Incorrect Resource Transfer Between Spheres	1471
HasMember	C	670	Always-Incorrect Control Flow Implementation	1475
HasMember	C	672	Operation on a Resource after Expiration or Release	1479
HasMember	C	674	Uncontrolled Recursion	1484
HasMember	P	682	Incorrect Calculation	1499
HasMember	P	697	Incorrect Comparison	1530
HasMember	C	704	Incorrect Type Conversion or Cast	1538
HasMember	C	706	Use of Incorrectly-Resolved Name or Reference	1544
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1551
HasMember	C	754	Improper Check for Unusual or Exceptional Conditions	1568
HasMember	C	755	Improper Handling of Exceptional Conditions	1576
HasMember	C	834	Excessive Iteration	1754
HasMember	C	862	Missing Authorization	1780
HasMember	C	863	Incorrect Authorization	1787
HasMember	C	913	Improper Control of Dynamically-Managed Code Resources	1805
HasMember	C	922	Insecure Storage of Sensitive Information	1825

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	938
Categories	0	out of	374
Views	0	out of	50
Total	130	out of	1362

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	2424
HasMember	C	1010	Authenticate Actors	2424
HasMember	C	1011	Authorize Actors	2425
HasMember	C	1012	Cross Cutting	2427
HasMember	C	1013	Encrypt Data	2428
HasMember	C	1014	Identify Actors	2429
HasMember	C	1015	Limit Access	2430
HasMember	C	1016	Limit Exposure	2431
HasMember	C	1017	Lock Computer	2431
HasMember	C	1018	Manage User Sessions	2432
HasMember	C	1019	Validate Inputs	2433
HasMember	C	1020	Verify Message Integrity	2434

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	938
Categories	12	out of	374
Views	0	out of	50
Total	235	out of	1362

View-1026: Weaknesses in OWASP Top Ten (2017)

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	2435
HasMember	C	1028	OWASP Top Ten 2017 Category A2 - Broken Authentication	2436
HasMember	C	1029	OWASP Top Ten 2017 Category A3 - Sensitive Data Exposure	2436
HasMember	C	1030	OWASP Top Ten 2017 Category A4 - XML External Entities (XXE)	2437
HasMember	C	1031	OWASP Top Ten 2017 Category A5 - Broken Access Control	2437
HasMember	C	1032	OWASP Top Ten 2017 Category A6 - Security Misconfiguration	2438
HasMember	C	1033	OWASP Top Ten 2017 Category A7 - Cross-Site Scripting (XSS)	2438
HasMember	C	1034	OWASP Top Ten 2017 Category A8 - Insecure Deserialization	2438
HasMember	C	1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities	2439
HasMember	C	1036	OWASP Top Ten 2017 Category A10 - Insufficient Logging & Monitoring	2439

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	938
Categories	12	out of	374

	CWEs in this view		Total CWEs
Views	0	out of	50
Total	53	out of	1362

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	2580

Metrics

	CWEs in this view		Total CWEs
Weaknesses	112	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	112	out of	1362

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	2580

Metrics

	CWEs in this view		Total CWEs
Weaknesses	143	out of	938
Categories	39	out of	374
Views	5	out of	50
Total	187	out of	1362

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	2440
HasMember	C	1130	CISQ Quality Measures (2016) - Maintainability	2441
HasMember	C	1131	CISQ Quality Measures (2016) - Security	2442
HasMember	C	1132	CISQ Quality Measures (2016) - Performance Efficiency	2443

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	938
Categories	4	out of	374
Views	0	out of	50
Total	81	out of	1362

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)	2444
HasMember	C	1135	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 01. Declarations and Initialization (DCL)	2444
HasMember	C	1136	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 02. Expressions (EXP)	2445
HasMember	C	1137	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 03. Numeric Types and Operations (NUM)	2445
HasMember	C	1138	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 04. Characters and Strings (STR)	2446
HasMember	C	1139	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 05. Object Orientation (OBJ)	2446
HasMember	C	1140	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 06. Methods (MET)	2447
HasMember	C	1141	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 07. Exceptional Behavior (ERR)	2448
HasMember	C	1142	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 08. Visibility and Atomicity (VNA)	2448

Nature	Type	ID	Name	Page
HasMember	C	1143	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 09. Locking (LCK)	2449
HasMember	C	1144	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 10. Thread APIs (THI)	2449
HasMember	C	1145	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 11. Thread Pools (TPS)	2450
HasMember	C	1146	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 12. Thread-Safety Miscellaneous (TSM)	2450
HasMember	C	1147	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 13. Input Output (FIO)	2450
HasMember	C	1148	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 14. Serialization (SER)	2451
HasMember	C	1149	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 15. Platform Security (SEC)	2452
HasMember	C	1150	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 16. Runtime Environment (ENV)	2452
HasMember	C	1151	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 17. Java Native Interface (JNI)	2453
HasMember	C	1152	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 49. Miscellaneous (MSC)	2453
HasMember	C	1153	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 50. Android (DRD)	2454
HasMember	C	1175	SEI CERT Oracle Secure Coding Standard for Java - Guidelines 18. Concurrency (CON)	2464

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	938
Categories	21	out of	374
Views	0	out of	50
Total	109	out of	1362

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)	2454
HasMember	C	1156	SEI CERT C Coding Standard - Guidelines 02. Declarations and Initialization (DCL)	2455
HasMember	C	1157	SEI CERT C Coding Standard - Guidelines 03. Expressions (EXP)	2455
HasMember	C	1158	SEI CERT C Coding Standard - Guidelines 04. Integers (INT)	2456
HasMember	C	1159	SEI CERT C Coding Standard - Guidelines 05. Floating Point (FLP)	2457
HasMember	C	1160	SEI CERT C Coding Standard - Guidelines 06. Arrays (ARR)	2457
HasMember	C	1161	SEI CERT C Coding Standard - Guidelines 07. Characters and Strings (STR)	2458
HasMember	C	1162	SEI CERT C Coding Standard - Guidelines 08. Memory Management (MEM)	2458
HasMember	C	1163	SEI CERT C Coding Standard - Guidelines 09. Input Output (FIO)	2459
HasMember	C	1165	SEI CERT C Coding Standard - Guidelines 10. Environment (ENV)	2460
HasMember	C	1166	SEI CERT C Coding Standard - Guidelines 11. Signals (SIG)	2460
HasMember	C	1167	SEI CERT C Coding Standard - Guidelines 12. Error Handling (ERR)	2461
HasMember	C	1168	SEI CERT C Coding Standard - Guidelines 13. Application Programming Interfaces (API)	2462
HasMember	C	1169	SEI CERT C Coding Standard - Guidelines 14. Concurrency (CON)	2462
HasMember	C	1170	SEI CERT C Coding Standard - Guidelines 48. Miscellaneous (MSC)	2463
HasMember	C	1171	SEI CERT C Coding Standard - Guidelines 50. POSIX (POS)	2463
HasMember	C	1172	SEI CERT C Coding Standard - Guidelines 51. Microsoft Windows (WIN)	2464

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	938
Categories	17	out of	374
Views	0	out of	50
Total	95	out of	1362

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)	2465
HasMember	C	1180	SEI CERT Perl Coding Standard - Guidelines 02. Declarations and Initialization (DCL)	2465
HasMember	C	1181	SEI CERT Perl Coding Standard - Guidelines 03. Expressions (EXP)	2466
HasMember	C	1182	SEI CERT Perl Coding Standard - Guidelines 04. Integers (INT)	2466
HasMember	C	1183	SEI CERT Perl Coding Standard - Guidelines 05. Strings (STR)	2467

Nature	Type	ID	Name	Page
HasMember	C	1184	SEI CERT Perl Coding Standard - Guidelines 06. Object-Oriented Programming (OOP)	2467
HasMember	C	1185	SEI CERT Perl Coding Standard - Guidelines 07. File Input and Output (FIO)	2468
HasMember	C	1186	SEI CERT Perl Coding Standard - Guidelines 50. Miscellaneous (MSC)	2468

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	938
Categories	9	out of	374
Views	0	out of	50
Total	35	out of	1362

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	2469
HasMember	C	1196	Security Flow Issues	2469
HasMember	C	1197	Integration Issues	2470
HasMember	C	1198	Privilege Separation and Access Control Issues	2470
HasMember	C	1199	General Circuit and Logic Design Concerns	2471

Nature	Type	ID	Name	Page
HasMember	C	1201	Core and Compute Issues	2471
HasMember	C	1202	Memory and Storage Issues	2472
HasMember	C	1203	Peripherals, On-chip Fabric, and Interface/IO Problems	2472
HasMember	C	1205	Security Primitives and Cryptography Issues	2473
HasMember	C	1206	Power, Clock, Thermal, and Reset Concerns	2473
HasMember	C	1207	Debug and Test Problems	2474
HasMember	C	1208	Cross-Cutting Problems	2474
HasMember	C	1388	Physical Access Issues and Concerns	2518

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	938
Categories	13	out of	374
Views	0	out of	50
Total	121	out of	1362

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')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	219
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	B	125	Out-of-bounds Read	330
HasMember	B	190	Integer Overflow or Wraparound	472
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	504
HasMember	C	269	Improper Privilege Management	646
HasMember	C	287	Improper Authentication	692
HasMember	B	295	Improper Certificate Validation	714
HasMember		352	Cross-Site Request Forgery (CSRF)	868
HasMember	C	400	Uncontrolled Resource Consumption	964
HasMember	V	416	Use After Free	1012
HasMember	B	426	Untrusted Search Path	1028
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	476	NULL Pointer Dereference	1132
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	B	611	Improper Restriction of XML External Entity Reference	1367
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1551
HasMember	B	772	Missing Release of Resource after Effective Lifetime	1624
HasMember	B	787	Out-of-bounds Write	1661
HasMember	B	798	Use of Hard-coded Credentials	1690

References

[REF-1028]"2019 CWE Top 25 Most Dangerous Software Errors". 2019 September 6. < http://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	25	out of	1362

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	2483
HasMember	C	1307	CISQ Quality Measures - Maintainability	2484
HasMember	C	1308	CISQ Quality Measures - Security	2485
HasMember	C	1309	CISQ Quality Measures - Efficiency	2486

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	938
Categories	4	out of	374
Views	0	out of	50
Total	142	out of	1362

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')	145
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	B	125	Out-of-bounds Read	330
HasMember	B	190	Integer Overflow or Wraparound	472
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	504
HasMember	B	276	Incorrect Default Permissions	665
HasMember	C	287	Improper Authentication	692
HasMember	B	306	Missing Authentication for Critical Function	741
HasMember	♣	352	Cross-Site Request Forgery (CSRF)	868
HasMember	V	416	Use After Free	1012
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	476	NULL Pointer Dereference	1132
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	C	522	Insufficiently Protected Credentials	1225
HasMember	B	611	Improper Restriction of XML External Entity Reference	1367
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1551
HasMember	B	787	Out-of-bounds Write	1661
HasMember	B	798	Use of Hard-coded Credentials	1690
HasMember	C	862	Missing Authorization	1780
HasMember	B	918	Server-Side Request Forgery (SSRF)	1820

References

[REF-1185]"2021 CWE Top 25 Most Dangerous Software Weaknesses". 2021 July 0. < http://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	25	out of	1362

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')	145
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	212
HasMember	B	91	XML Injection (aka Blind XPath Injection)	215
HasMember	C	99	Improper Control of Resource Identifiers ('Resource Injection')	243
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	V	129	Improper Validation of Array Index	341
HasMember	B	134	Use of Externally-Controlled Format String	365
HasMember	B	170	Improper Null Termination	428
HasMember	B	213	Exposure of Sensitive Information Due to Incompatible Policies	547
HasMember	P	284	Improper Access Control	680
HasMember	C	311	Missing Encryption of Sensitive Data	757
HasMember	B	359	Exposure of Private Personal Information to an Unauthorized Actor	882
HasMember	C	404	Improper Resource Shutdown or Release	980
HasMember	C	424	Improper Protection of Alternate Path	1023
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	B	562	Return of Stack Variable Address	1278
HasMember	B	606	Unchecked Input for Loop Condition	1357
HasMember	B	611	Improper Restriction of XML External Entity Reference	1367

Nature	Type	ID	Name	Page
HasMember	B	643	Improper Neutralization of Data within XPath Expressions ('XPath Injection')	1419
HasMember	B	652	Improper Neutralization of Data within XQuery Expressions ('XQuery Injection')	1435
HasMember	C	662	Improper Synchronization	1448
HasMember	C	665	Improper Initialization	1456
HasMember	C	672	Operation on a Resource after Expiration or Release	1479
HasMember	B	681	Incorrect Conversion between Numeric Types	1495
HasMember	P	682	Incorrect Calculation	1499
HasMember	P	703	Improper Check or Handling of Exceptional Conditions	1535
HasMember	C	704	Incorrect Type Conversion or Cast	1538
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1551
HasMember	B	798	Use of Hard-coded Credentials	1690
HasMember	B	908	Use of Uninitialized Resource	1792
HasMember	B	915	Improperly Controlled Modification of Dynamically-Determined Object Attributes	1809
HasMember	B	1051	Initialization with Hard-Coded Network Resource Configuration Data	1886

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	938
Categories	0	out of	374
Views	0	out of	50
Total	89	out of	1362

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)	1976
HasMember	B	1191	On-Chip Debug and Test Interface With Improper Access Control	1980
HasMember	B	1231	Improper Prevention of Lock Bit Modification	2007
HasMember	B	1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection	2012
HasMember	B	1240	Use of a Cryptographic Primitive with a Risky Implementation	2025
HasMember	B	1244	Internal Asset Exposed to Unsafe Debug Access Level or State	2037
HasMember	B	1256	Improper Restriction of Software Interfaces to Hardware Features	2065
HasMember	B	1260	Improper Handling of Overlap Between Protected Memory Ranges	2075
HasMember	B	1272	Sensitive Information Uncleared Before Debug/Power State Transition	2104
HasMember	B	1274	Improper Access Control for Volatile Memory Containing Boot Code	2108
HasMember	B	1277	Firmware Not Updateable	2116
HasMember	B	1300	Improper Protection of Physical Side Channels	2165

References

[REF-1238]MITRE. "2021 CWE Most Important Hardware Weaknesses". 2021 October 8. < https://cwe.mitre.org/scoring/lists/2021_CWE_MiHW.html >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	12	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	12	out of	1362

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	2487
HasMember	C	1346	OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures	2488
HasMember	C	1347	OWASP Top Ten 2021 Category A03:2021 - Injection	2490
HasMember	C	1348	OWASP Top Ten 2021 Category A04:2021 - Insecure Design	2491
HasMember	C	1349	OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration	2493
HasMember	C	1352	OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components	2494
HasMember	C	1353	OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures	2494
HasMember	C	1354	OWASP Top Ten 2021 Category A08:2021 - Software and Data Integrity Failures	2495
HasMember	C	1355	OWASP Top Ten 2021 Category A09:2021 - Security Logging and Monitoring Failures	2496
HasMember	C	1356	OWASP Top Ten 2021 Category A10:2021 - Server-Side Request Forgery (SSRF)	2497

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	938
Categories	23	out of	374
Views	0	out of	50
Total	205	out of	1362

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')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	219
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	B	125	Out-of-bounds Read	330
HasMember	B	190	Integer Overflow or Wraparound	472
HasMember	C	200	Exposure of Sensitive Information to an Unauthorized Actor	504
HasMember	C	269	Improper Privilege Management	646
HasMember	C	287	Improper Authentication	692
HasMember	B	306	Missing Authentication for Critical Function	741
HasMember		352	Cross-Site Request Forgery (CSRF)	868
HasMember	C	400	Uncontrolled Resource Consumption	964
HasMember	V	416	Use After Free	1012
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	476	NULL Pointer Dereference	1132
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	C	522	Insufficiently Protected Credentials	1225
HasMember	B	611	Improper Restriction of XML External Entity Reference	1367
HasMember	C	732	Incorrect Permission Assignment for Critical Resource	1551
HasMember	B	787	Out-of-bounds Write	1661
HasMember	B	798	Use of Hard-coded Credentials	1690
HasMember	C	862	Missing Authorization	1780

References

[REF-1132]"2020 CWE Top 25 Most Dangerous Software Weaknesses". 2020 August 0. < http://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	938
Categories	0	out of	374

	CWEs in this view		Total CWEs
Views	0	out of	50
Total	25	out of	1362

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	2497
HasMember	C	1360	ICS Dependencies (& Architecture)	2498
HasMember	C	1361	ICS Supply Chain	2499
HasMember	C	1362	ICS Engineering (Constructions/Deployment)	2499
HasMember	C	1363	ICS Operations (& Maintenance)	2500

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	938
Categories	26	out of	374
Views	0	out of	50
Total	107	out of	1362

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')	145
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	219
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293

Nature	Type	ID	Name	Page
HasMember	B	125	Out-of-bounds Read	330
HasMember	B	190	Integer Overflow or Wraparound	472
HasMember	B	276	Incorrect Default Permissions	665
HasMember	C	287	Improper Authentication	692
HasMember	B	306	Missing Authentication for Critical Function	741
HasMember		352	Cross-Site Request Forgery (CSRF)	868
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	888
HasMember	C	400	Uncontrolled Resource Consumption	964
HasMember	V	416	Use After Free	1012
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	476	NULL Pointer Dereference	1132
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	B	611	Improper Restriction of XML External Entity Reference	1367
HasMember	B	787	Out-of-bounds Write	1661
HasMember	B	798	Use of Hard-coded Credentials	1690
HasMember	C	862	Missing Authorization	1780
HasMember	B	918	Server-Side Request Forgery (SSRF)	1820

References

[REF-1268]"2022 CWE Top 25 Most Dangerous Software Weaknesses". 2022 June 8. < http://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html >.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	25	out of	1362

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	2519
HasMember	C	1397	Comprehensive Categorization: Comparison	2523
HasMember	C	1398	Comprehensive Categorization: Component Interaction	2524
HasMember	C	1399	Comprehensive Categorization: Memory Safety	2525
HasMember	C	1401	Comprehensive Categorization: Concurrency	2526
HasMember	C	1402	Comprehensive Categorization: Encryption	2527
HasMember	C	1403	Comprehensive Categorization: Exposed Resource	2528
HasMember	C	1404	Comprehensive Categorization: File Handling	2529
HasMember	C	1405	Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions	2531
HasMember	C	1406	Comprehensive Categorization: Improper Input Validation	2531
HasMember	C	1407	Comprehensive Categorization: Improper Neutralization	2532
HasMember	C	1408	Comprehensive Categorization: Incorrect Calculation	2534
HasMember	C	1409	Comprehensive Categorization: Injection	2535
HasMember	C	1410	Comprehensive Categorization: Insufficient Control Flow Management	2536
HasMember	C	1411	Comprehensive Categorization: Insufficient Verification of Data Authenticity	2538
HasMember	C	1412	Comprehensive Categorization: Poor Coding Practices	2538
HasMember	C	1413	Comprehensive Categorization: Protection Mechanism Failure	2542
HasMember	C	1414	Comprehensive Categorization: Randomness	2543
HasMember	C	1415	Comprehensive Categorization: Resource Control	2544
HasMember	C	1416	Comprehensive Categorization: Resource Lifecycle Management	2545
HasMember	C	1417	Comprehensive Categorization: Sensitive Information Exposure	2548
HasMember	C	1418	Comprehensive Categorization: Violation of Secure Design Principles	2549

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	938	out of	938
Categories	22	out of	374
Views	0	out of	50
Total	960	out of	1362

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	2600

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	938
Categories	0	out of	374
Views	0	out of	50
Total	39	out of	1362

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')	145
HasMember	B	78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	151
HasMember	B	79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	163
HasMember	B	89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	201
HasMember	B	94	Improper Control of Generation of Code ('Code Injection')	219
HasMember	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer	293
HasMember	B	125	Out-of-bounds Read	330
HasMember	B	190	Integer Overflow or Wraparound	472
HasMember	C	269	Improper Privilege Management	646
HasMember	B	276	Incorrect Default Permissions	665
HasMember	C	287	Improper Authentication	692
HasMember	B	306	Missing Authentication for Critical Function	741
HasMember	♣	352	Cross-Site Request Forgery (CSRF)	868
HasMember	C	362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	888
HasMember	V	416	Use After Free	1012
HasMember	B	434	Unrestricted Upload of File with Dangerous Type	1048
HasMember	B	476	NULL Pointer Dereference	1132
HasMember	B	502	Deserialization of Untrusted Data	1204
HasMember	B	787	Out-of-bounds Write	1661
HasMember	B	798	Use of Hard-coded Credentials	1690
HasMember	C	862	Missing Authorization	1780
HasMember	C	863	Incorrect Authorization	1787
HasMember	B	918	Server-Side Request Forgery (SSRF)	1820

References

[REF-1344]"2023 CWE Top 25 Most Dangerous Software Weaknesses". 2023 June 9. < http://cwe.mitre.org/top25/archive/2023/2023_cwe_top25.html >.2023-06-29.

Metrics

	CWEs in this view		Total CWEs
Weaknesses	25	out of	938
Categories	0	out of	374
Views	0	out of	50
Total	25	out of	1362

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	2601

Metrics

	CWEs in this view		Total CWEs
Weaknesses	938	out of	938
Categories	374	out of	374
Views	50	out of	50
Total	1362	out of	1362

Graph View: CWE-629: Weaknesses in OWASP Top Ten (2007)

- CWE-712: OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS) *(p.2330)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-713: OWASP Top Ten 2007 Category A2 - Injection Flaws *(p.2330)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
  - CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
- CWE-714: OWASP Top Ten 2007 Category A3 - Malicious File Execution *(p.2331)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
  - CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*
- CWE-715: OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference *(p.2331)*
  - 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.1123)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
- CWE-716: OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF) *(p.2331)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-717: OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling *(p.2332)*
  - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
  - CWE-203: Observable Discrepancy *(p.518)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
- CWE-718: OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management *(p.2332)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.733)*
  - CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-719: OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage *(p.2333)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
- CWE-720: OWASP Top Ten 2007 Category A9 - Insecure Communications *(p.2333)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
- CWE-721: OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access *(p.2333)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*

Graph View: CWE-631: DEPRECATED: Resource-specific Weaknesses

Graph View: CWE-699: Software Development

- CWE-1228: API / Function Errors *(p.2482)*
  - CWE-242: Use of Inherently Dangerous Function *(p.586)*
  - CWE-474: Use of Function with Inconsistent Implementations *(p.1128)*
  - CWE-475: Undefined Behavior for Input to API *(p.1130)*
  - CWE-477: Use of Obsolete Function *(p.1138)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1489)*
  - CWE-695: Use of Low-Level Functionality *(p.1524)*
  - CWE-749: Exposed Dangerous Method or Function *(p.1564)*
- CWE-1210: Audit / Logging Errors *(p.2475)*
  - CWE-117: Improper Output Neutralization for Logs *(p.288)*
  - CWE-222: Truncation of Security-relevant Information *(p.557)*
  - CWE-223: Omission of Security-relevant Information *(p.559)*
  - CWE-224: Obscured Security-relevant Information by Alternate Name *(p.561)*
  - CWE-778: Insufficient Logging *(p.1638)*
  - CWE-779: Logging of Excessive Data *(p.1642)*
- CWE-1211: Authentication Errors *(p.2475)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.703)*
  - CWE-290: Authentication Bypass by Spoofing *(p.705)*
  - CWE-294: Authentication Bypass by Capture-replay *(p.712)*
  - CWE-295: Improper Certificate Validation *(p.714)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.733)*
  - CWE-303: Incorrect Implementation of Authentication Algorithm *(p.737)*
  - CWE-305: Authentication Bypass by Primary Weakness *(p.740)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-308: Use of Single-factor Authentication *(p.752)*
  - CWE-309: Use of Password System for Primary Authentication *(p.754)*
  - CWE-322: Key Exchange without Entity Authentication *(p.788)*
  - CWE-603: Use of Client-Side Authentication *(p.1354)*
  - CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1423)*
  - CWE-804: Guessable CAPTCHA *(p.1701)*
  - CWE-836: Use of Password Hash Instead of Password for Authentication *(p.1761)*
- CWE-1212: Authorization Errors *(p.2476)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
  - CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
  - CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
  - CWE-939: Improper Authorization in Handler for Custom URL Scheme *(p.1840)*
  - CWE-842: Placement of User into Incorrect Group *(p.1775)*
  - CWE-1220: Insufficient Granularity of Access Control *(p.1992)*
  - CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2006)*
- CWE-1006: Bad Coding Practices *(p.2422)*
  - CWE-358: Improperly Implemented Security Check for Standard *(p.881)*
  - CWE-360: Trust of System Event Data *(p.887)*
  - CWE-478: Missing Default Case in Multiple Condition Expression *(p.1142)*
  - CWE-487: Reliance on Package-level Scope *(p.1167)*
  - CWE-489: Active Debug Code *(p.1171)*
  - CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1259)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-562: Return of Stack Variable Address *(p.1278)*
  - CWE-563: Assignment to Variable without Use *(p.1280)*
  - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*

- CWE-438: Behavioral Problems *(p.2326)*
  - CWE-115: Misinterpretation of Input *(p.280)*
  - CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
  - CWE-408: Incorrect Behavior Order: Early Amplification *(p.995)*
  - CWE-437: Incomplete Model of Endpoint Features *(p.1059)*
  - CWE-439: Behavioral Change in New Version or Environment *(p.1061)*
  - CWE-440: Expected Behavior Violation *(p.1062)*
  - CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1068)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
  - CWE-483: Incorrect Block Delimitation *(p.1160)*
  - CWE-484: Omitted Break Statement in Switch *(p.1162)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
  - CWE-698: Execution After Redirect (EAR) *(p.1533)*
  - CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1562)*
  - CWE-783: Operator Precedence Logic Error *(p.1650)*
  - CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*
  - CWE-837: Improper Enforcement of a Single, Unique Action *(p.1762)*
  - CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*
  - CWE-1025: Comparison Using Wrong Factors *(p.1868)*
  - CWE-1037: Processor Optimization Removal or Modification of Security-critical Code *(p.1870)*
- CWE-840: Business Logic Errors *(p.2360)*
  - CWE-283: Unverified Ownership *(p.678)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
  - CWE-708: Incorrect Ownership Assignment *(p.1548)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
  - CWE-826: Premature Release of Resource During Expected Lifetime *(p.1734)*
  - CWE-837: Improper Enforcement of a Single, Unique Action *(p.1762)*
  - CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*
- CWE-417: Communication Channel Errors *(p.2325)*
  - CWE-322: Key Exchange without Entity Authentication *(p.788)*
  - CWE-346: Origin Validation Error *(p.853)*
  - CWE-385: Covert Timing Channel *(p.940)*
  - CWE-419: Unprotected Primary Channel *(p.1017)*
  - CWE-420: Unprotected Alternate Channel *(p.1018)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-515: Covert Storage Channel *(p.1220)*
  - CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*
  - CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1830)*
  - CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*
  - CWE-941: Incorrectly Specified Destination in a Communication Channel *(p.1845)*
  - CWE-1327: Binding to an Unrestricted IP Address *(p.2215)*
- CWE-1226: Complexity Issues *(p.2481)*
  - CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1877)*
  - CWE-1047: Modules with Circular Dependencies *(p.1882)*
  - CWE-1055: Multiple Inheritance from Concrete Classes *(p.1890)*
  - CWE-1056: Invokable Control Element with Variadic Parameters *(p.1891)*
  - CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses *(p.1897)*
  - CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters *(p.1902)*
  - CWE-1074: Class with Excessively Deep Inheritance *(p.1914)*
  - CWE-1075: Unconditional Control Flow Transfer outside of Switch Block *(p.1915)*

- B CWE-1080: Source Code File with Excessive Number of Lines of Code *(p.1920)*
- B CWE-1086: Class with Excessive Number of Child Classes *(p.1926)*
- B CWE-1095: Loop Condition Value Update within the Loop *(p.1935)*
- B CWE-1119: Excessive Use of Unconditional Branching *(p.1959)*
- B CWE-1121: Excessive McCabe Cyclomatic Complexity *(p.1961)*
- B CWE-1122: Excessive Halstead Complexity *(p.1962)*
- B CWE-1123: Excessive Use of Self-Modifying Code *(p.1963)*
- B CWE-1124: Excessively Deep Nesting *(p.1964)*
- B CWE-1125: Excessive Attack Surface *(p.1965)*
- B CWE-1333: Inefficient Regular Expression Complexity *(p.2230)*

C CWE-557: Concurrency Issues *(p.2329)*
- B CWE-364: Signal Handler Race Condition *(p.899)*
- B CWE-366: Race Condition within a Thread *(p.904)*
- B CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
- B CWE-368: Context Switching Race Condition *(p.912)*
- B CWE-386: Symbolic Name not Mapping to Correct Object *(p.942)*
- B CWE-421: Race Condition During Access to Alternate Channel *(p.1020)*
- B CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1452)*
- B CWE-820: Missing Synchronization *(p.1720)*
- B CWE-821: Incorrect Synchronization *(p.1722)*
- B CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
- B CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context *(p.2207)*

C CWE-255: Credentials Management Errors *(p.2315)*
- B CWE-256: Plaintext Storage of a Password *(p.615)*
- B CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
- B CWE-260: Password in Configuration File *(p.629)*
- B CWE-261: Weak Encoding for Password *(p.631)*
- B CWE-262: Not Using Password Aging *(p.633)*
- B CWE-263: Password Aging with Long Expiration *(p.636)*
- B CWE-324: Use of a Key Past its Expiration Date *(p.792)*
- B CWE-521: Weak Password Requirements *(p.1223)*
- B CWE-523: Unprotected Transport of Credentials *(p.1230)*
- B CWE-549: Missing Password Field Masking *(p.1262)*
- B CWE-620: Unverified Password Change *(p.1383)*
- B CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- B CWE-798: Use of Hard-coded Credentials *(p.1690)*
- B CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
- B CWE-1392: Use of Default Credentials *(p.2271)*

C CWE-310: Cryptographic Issues *(p.2318)*
- B CWE-261: Weak Encoding for Password *(p.631)*
- B CWE-324: Use of a Key Past its Expiration Date *(p.792)*
- B CWE-325: Missing Cryptographic Step *(p.794)*
- B CWE-328: Use of Weak Hash *(p.806)*
- B CWE-331: Insufficient Entropy *(p.821)*
- B CWE-334: Small Space of Random Values *(p.827)*
- B CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
- B CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- B CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- B CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
- B CWE-1204: Generation of Weak Initialization Vector (IV) *(p.1987)*
- B CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation *(p.2025)*

C CWE-320: Key Management Errors *(p.2319)*
- B CWE-322: Key Exchange without Entity Authentication *(p.788)*

- CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.790)*
- CWE-324: Use of a Key Past its Expiration Date *(p.792)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*

CWE-1214: Data Integrity Issues *(p.2477)*

- CWE-322: Key Exchange without Entity Authentication *(p.788)*
- CWE-346: Origin Validation Error *(p.853)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- CWE-348: Use of Less Trusted Source *(p.859)*
- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- CWE-351: Insufficient Type Distinction *(p.866)*
- CWE-353: Missing Support for Integrity Check *(p.874)*
- CWE-354: Improper Validation of Integrity Check Value *(p.876)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
- CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1430)*
- CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
- CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1830)*

CWE-19: Data Processing Errors *(p.2309)*

- CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
- CWE-166: Improper Handling of Missing Special Element *(p.423)*
- CWE-167: Improper Handling of Additional Special Element *(p.425)*
- CWE-168: Improper Handling of Inconsistent Special Elements *(p.426)*
- CWE-178: Improper Handling of Case Sensitivity *(p.445)*
- CWE-182: Collapse of Data into Unsafe Value *(p.455)*
- CWE-186: Overly Restrictive Regular Expression *(p.466)*
- CWE-229: Improper Handling of Values *(p.570)*
- CWE-233: Improper Handling of Parameters *(p.574)*
- CWE-237: Improper Handling of Structural Elements *(p.580)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.996)*
- CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-624: Executable Regular Expression Error *(p.1390)*
- CWE-625: Permissive Regular Expression *(p.1392)*
- CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*
- CWE-1024: Comparison of Incompatible Types *(p.1867)*

CWE-137: Data Neutralization Issues *(p.2311)*

- CWE-76: Improper Neutralization of Equivalent Special Elements *(p.144)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-117: Improper Output Neutralization for Logs *(p.288)*
- CWE-140: Improper Neutralization of Delimiters *(p.376)*

- CWE-170: Improper Null Termination *(p.428)*
- CWE-463: Deletion of Data Structure Sentinel *(p.1105)*
- CWE-464: Addition of Data Structure Sentinel *(p.1107)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1412)*
- CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1523)*
- CWE-791: Incomplete Filtering of Special Elements *(p.1680)*
- CWE-838: Inappropriate Encoding for Output Context *(p.1764)*
- CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
- CWE-1236: Improper Neutralization of Formula Elements in a CSV File *(p.2019)*

CWE-1225: Documentation Issues *(p.2480)*
- CWE-1053: Missing Documentation for Design *(p.1888)*
- CWE-1068: Inconsistency Between Implementation and Documented Design *(p.1906)*
- CWE-1110: Incomplete Design Documentation *(p.1950)*
- CWE-1111: Incomplete I/O Documentation *(p.1951)*
- CWE-1112: Incomplete Documentation of Program Execution *(p.1952)*
- CWE-1118: Insufficient Documentation of Error Handling Techniques *(p.1958)*

CWE-1219: File Handling Issues *(p.2480)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-41: Improper Resolution of Path Equivalence *(p.86)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
- CWE-66: Improper Handling of File Names that Identify Virtual Resources *(p.124)*
- CWE-378: Creation of Temporary File With Insecure Permissions *(p.928)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.930)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-427: Uncontrolled Search Path Element *(p.1033)*
- CWE-428: Unquoted Search Path or Element *(p.1039)*

CWE-1227: Encapsulation Issues *(p.2481)*
- CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer *(p.1889)*
- CWE-1057: Data Access Operations Outside of Expected Data Manager Component *(p.1892)*
- CWE-1062: Parent Class with References to Child Class *(p.1900)*
- CWE-1083: Data Access from Outside Expected Data Manager Component *(p.1922)*
- CWE-1090: Method Containing Access of a Member Element from Another Class *(p.1930)*
- CWE-1100: Insufficient Isolation of System-Dependent Functions *(p.1940)*
- CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality *(p.1945)*

CWE-389: Error Conditions, Return Values, Status Codes *(p.2322)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-248: Uncaught Exception *(p.596)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-253: Incorrect Check of Function Return Value *(p.613)*
- CWE-390: Detection of Error Condition Without Action *(p.943)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-392: Missing Report of Error Condition *(p.951)*
- CWE-393: Return of Wrong Status Code *(p.953)*
- CWE-394: Unexpected Status Code or Return Value *(p.955)*
- CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.957)*
- CWE-396: Declaration of Catch for Generic Exception *(p.959)*
- CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-544: Missing Standardized Error Handling Mechanism *(p.1256)*
- CWE-584: Return Inside Finally Block *(p.1317)*
- CWE-617: Reachable Assertion *(p.1378)*
- CWE-756: Missing Custom Error Page *(p.1579)*

CWE-569: Expression Issues *(p.2330)*
- CWE-480: Use of Incorrect Operator *(p.1150)*

- CWE-570: Expression is Always False *(p.1292)*
- CWE-571: Expression is Always True *(p.1295)*
- CWE-783: Operator Precedence Logic Error *(p.1650)*

CWE-429: Handler Errors *(p.2326)*
- CWE-430: Deployment of Wrong Handler *(p.1042)*
- CWE-431: Missing Handler *(p.1043)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*

CWE-199: Information Management Errors *(p.2312)*
- CWE-201: Insertion of Sensitive Information Into Sent Data *(p.514)*
- CWE-204: Observable Response Discrepancy *(p.523)*
- CWE-205: Observable Behavioral Discrepancy *(p.526)*
- CWE-208: Observable Timing Discrepancy *(p.529)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
- CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.547)*
- CWE-214: Invocation of Process Using Visible Sensitive Information *(p.549)*
- CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
- CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
- CWE-524: Use of Cache Containing Sensitive Information *(p.1232)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
- CWE-921: Storage of Sensitive Data in a Mechanism without Access Control *(p.1824)*
- CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2006)*

CWE-452: Initialization and Cleanup Errors *(p.2327)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
- CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1085)*
- CWE-455: Non-exit on Failed Initialization *(p.1087)*
- CWE-459: Incomplete Cleanup *(p.1099)*
- CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
- CWE-1052: Excessive Use of Hard-Coded Literals in Initialization *(p.1887)*
- CWE-1188: Initialization of a Resource with an Insecure Default *(p.1974)*

CWE-1215: Data Validation Issues *(p.2478)*
- CWE-112: Missing XML Validation *(p.269)*
- CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
- CWE-183: Permissive List of Allowed Inputs *(p.458)*
- CWE-184: Incomplete List of Disallowed Inputs *(p.459)*
- CWE-606: Unchecked Input for Loop Condition *(p.1357)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1412)*
- CWE-1173: Improper Use of Validation Framework *(p.1969)*
- CWE-1284: Improper Validation of Specified Quantity in Input *(p.2130)*
- CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input *(p.2132)*
- CWE-1286: Improper Validation of Syntactic Correctness of Input *(p.2136)*
- CWE-1287: Improper Validation of Specified Type of Input *(p.2138)*
- CWE-1288: Improper Validation of Consistency within Input *(p.2139)*
- CWE-1289: Improper Validation of Unsafe Equivalence in Input *(p.2141)*

CWE-1216: Lockout Mechanism Errors *(p.2478)*
- CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1423)*

CWE-1218: Memory Buffer Errors *(p.2479)*
- CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
- CWE-124: Buffer Underwrite ('Buffer Underflow') *(p.326)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.355)*

- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-341: Predictable from Observable State *(p.843)*
- CWE-342: Predictable Exact Value from Previous Values *(p.845)*
- CWE-343: Predictable Value Range from Previous Values *(p.847)*
- CWE-344: Use of Invariant Value in Dynamically Changing Context *(p.849)*
- CWE-1241: Use of Predictable Algorithm in Random Number Generator *(p.2030)*

CWE-411: Resource Locking Problems *(p.2325)*
- CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
- CWE-413: Improper Resource Locking *(p.1003)*
- CWE-414: Missing Lock Check *(p.1007)*
- CWE-609: Double-Checked Locking *(p.1362)*
- CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
- CWE-765: Multiple Unlocks of a Critical Resource *(p.1605)*
- CWE-832: Unlock of a Resource that is not Locked *(p.1752)*
- CWE-833: Deadlock *(p.1753)*

CWE-399: Resource Management Errors *(p.2324)*
- CWE-73: External Control of File Name or Path *(p.132)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
- CWE-410: Insufficient Resource Pool *(p.998)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-619: Dangling Database Cursor ('Cursor Injection') *(p.1382)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1412)*
- CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1523)*
- CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-771: Missing Reference to Active Allocated Resource *(p.1622)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-826: Premature Release of Resource During Expected Lifetime *(p.1734)*
- CWE-908: Use of Uninitialized Resource *(p.1792)*
- CWE-909: Missing Initialization of Resource *(p.1797)*
- CWE-910: Use of Expired File Descriptor *(p.1800)*
- CWE-911: Improper Update of Reference Count *(p.1801)*
- CWE-914: Improper Control of Dynamically-Identified Variables *(p.1807)*
- CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes *(p.1809)*
- CWE-920: Improper Restriction of Power Consumption *(p.1823)*
- CWE-1188: Initialization of a Resource with an Insecure Default *(p.1974)*
- CWE-1341: Multiple Releases of Same Resource or Handle *(p.2246)*

CWE-387: Signal Errors *(p.2321)*
- CWE-364: Signal Handler Race Condition *(p.899)*

CWE-371: State Issues *(p.2321)*
- CWE-15: External Control of System or Configuration Setting *(p.17)*
- CWE-372: Incomplete Internal State Distinction *(p.919)*
- CWE-374: Passing Mutable Objects to an Untrusted Method *(p.920)*
- CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
- CWE-1265: Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls *(p.2088)*

CWE-133: String Errors *(p.2310)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.370)*
- CWE-480: Use of Incorrect Operator *(p.1150)*

CWE-136: Type Errors *(p.2310)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') *(p.1776)*

- B CWE-1287: Improper Validation of Specified Type of Input *(p.2138)*
- C CWE-355: User Interface Security Issues *(p.2320)*
  - B CWE-356: Product UI does not Warn User of Unsafe Actions *(p.879)*
  - B CWE-357: Insufficient UI Warning of Dangerous Operations *(p.880)*
  - B CWE-447: Unimplemented or Unsupported Feature in UI *(p.1075)*
  - B CWE-448: Obsolete Feature in UI *(p.1076)*
  - B CWE-449: The UI Performs the Wrong Action *(p.1077)*
  - B CWE-549: Missing Password Field Masking *(p.1262)*
  - B CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User *(p.1857)*
  - B CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
- C CWE-1217: User Session Errors *(p.2479)*
  - B CWE-488: Exposure of Data Element to Wrong Session *(p.1169)*
  - B CWE-613: Insufficient Session Expiration *(p.1371)*
  - B CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*

Graph View: CWE-700: Seven Pernicious Kingdoms

- CWE-254: 7PK - Security Features *(p.2314)*
  - CWE-256: Plaintext Storage of a Password *(p.615)*
  - CWE-258: Empty Password in Configuration File *(p.621)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-260: Password in Configuration File *(p.629)*
  - CWE-261: Weak Encoding for Password *(p.631)*
  - CWE-272: Least Privilege Violation *(p.656)*
  - CWE-284: Improper Access Control *(p.680)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-361: 7PK - Time and State *(p.2320)*
  - CWE-364: Signal Handler Race Condition *(p.899)*
  - CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
  - CWE-377: Insecure Temporary File *(p.925)*
  - CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
  - CWE-383: J2EE Bad Practices: Direct Use of Threads *(p.935)*
  - CWE-384: Session Fixation *(p.936)*
  - CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
- CWE-388: 7PK - Errors *(p.2322)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.957)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.959)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-1005: 7PK - Input Validation and Representation *(p.2421)*
  - CWE-20: Improper Input Validation *(p.20)*
    - CWE-102: Struts: Duplicate Validation Forms *(p.246)*
    - CWE-103: Struts: Incomplete validate() Method Definition *(p.248)*
    - CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.251)*
    - CWE-105: Struts: Form Field Without Validator *(p.253)*
    - CWE-106: Struts: Plug-in Framework not in Use *(p.256)*
    - CWE-107: Struts: Unused Validation Form *(p.259)*
    - CWE-108: Struts: Unvalidated Action Form *(p.261)*
    - CWE-109: Struts: Validator Turned Off *(p.263)*
    - CWE-110: Struts: Validator Without Form Field *(p.264)*
    - CWE-111: Direct Use of Unsafe JNI *(p.266)*
    - CWE-112: Missing XML Validation *(p.269)*
    - CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.271)*
    - CWE-114: Process Control *(p.277)*
    - CWE-117: Improper Output Neutralization for Logs *(p.288)*
    - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
    - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
    - CWE-134: Use of Externally-Controlled Format String *(p.365)*
    - CWE-15: External Control of System or Configuration Setting *(p.17)*
    - CWE-170: Improper Null Termination *(p.428)*
    - CWE-190: Integer Overflow or Wraparound *(p.472)*
    - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1109)*
    - CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
    - CWE-73: External Control of File Name or Path *(p.132)*
    - CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer *(p.1656)*

- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*

CWE-227: 7PK - API Abuse *(p.2313)*
- CWE-242: Use of Inherently Dangerous Function *(p.586)*
- CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.589)*
- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
- CWE-245: J2EE Bad Practices: Direct Management of Connections *(p.592)*
- CWE-246: J2EE Bad Practices: Direct Use of Sockets *(p.594)*
- CWE-248: Uncaught Exception *(p.596)*
- CWE-250: Execution with Unnecessary Privileges *(p.599)*
- CWE-251: Often Misused: String Management *(p.2314)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-558: Use of getlogin() in Multithreaded Application *(p.1272)*

CWE-398: 7PK - Code Quality *(p.2323)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-415: Double Free *(p.1008)*
- CWE-416: Use After Free *(p.1012)*
- CWE-457: Use of Uninitialized Variable *(p.1094)*
- CWE-474: Use of Function with Inconsistent Implementations *(p.1128)*
- CWE-475: Undefined Behavior for Input to API *(p.1130)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-477: Use of Obsolete Function *(p.1138)*

CWE-485: 7PK - Encapsulation *(p.2328)*
- CWE-486: Comparison of Classes by Name *(p.1164)*
- CWE-488: Exposure of Data Element to Wrong Session *(p.1169)*
- CWE-489: Active Debug Code *(p.1171)*
- CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1174)*
- CWE-492: Use of Inner Class Containing Sensitive Data *(p.1175)*
- CWE-493: Critical Public Variable Without Final Modifier *(p.1182)*
- CWE-495: Private Data Structure Returned From A Public Method *(p.1189)*
- CWE-496: Public Data Assigned to Private Array-Typed Field *(p.1192)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
- CWE-501: Trust Boundary Violation *(p.1203)*

CWE-2: 7PK - Environment *(p.2308)*
- 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.2334)*
  - CWE-102: Struts: Duplicate Validation Forms *(p.246)*
  - CWE-103: Struts: Incomplete validate() Method Definition *(p.248)*
  - CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.251)*
  - CWE-106: Struts: Plug-in Framework not in Use *(p.256)*
  - CWE-109: Struts: Validator Turned Off *(p.263)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-166: Improper Handling of Missing Special Element *(p.423)*
  - CWE-167: Improper Handling of Additional Special Element *(p.425)*
  - CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
  - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
  - CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.453)*
  - CWE-182: Collapse of Data into Unsafe Value *(p.455)*
  - CWE-183: Permissive List of Allowed Inputs *(p.458)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
  - CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-723: OWASP Top Ten 2004 Category A2 - Broken Access Control *(p.2335)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-266: Incorrect Privilege Assignment *(p.638)*
  - CWE-268: Privilege Chaining *(p.644)*
  - CWE-275: Permission Issues *(p.2317)*
  - CWE-283: Unverified Ownership *(p.678)*
  - CWE-284: Improper Access Control *(p.680)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-41: Improper Resolution of Path Equivalence *(p.86)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1233)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
  - CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1271)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
  - CWE-708: Incorrect Ownership Assignment *(p.1548)*
  - CWE-73: External Control of File Name or Path *(p.132)*
  - 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.2335)*
  - CWE-255: Credentials Management Errors *(p.2315)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
  - CWE-298: Improper Validation of Certificate Expiration *(p.726)*
  - CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
  - CWE-304: Missing Critical Step in Authentication *(p.738)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*

- CWE-309: Use of Password System for Primary Authentication *(p.754)*
- CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
- CWE-384: Session Fixation *(p.936)*
- CWE-521: Weak Password Requirements *(p.1223)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1233)*
- CWE-613: Insufficient Session Expiration *(p.1371)*
- CWE-620: Unverified Password Change *(p.1383)*
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*

CWE-725: OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws *(p.2336)*
- CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(p.1422)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*

CWE-726: OWASP Top Ten 2004 Category A5 - Buffer Overflows *(p.2336)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*

CWE-727: OWASP Top Ten 2004 Category A6 - Injection Flaws *(p.2337)*
- CWE-117: Improper Output Neutralization for Logs *(p.288)*
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
- CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*

CWE-728: OWASP Top Ten 2004 Category A7 - Improper Error Handling *(p.2337)*
- CWE-203: Observable Discrepancy *(p.518)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.568)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-389: Error Conditions, Return Values, Status Codes *(p.2322)*
- CWE-390: Detection of Error Condition Without Action *(p.943)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-394: Unexpected Status Code or Return Value *(p.955)*
- CWE-636: Not Failing Securely ('Failing Open') *(p.1401)*
- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*

CWE-729: OWASP Top Ten 2004 Category A8 - Insecure Storage *(p.2338)*
- CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
- CWE-261: Weak Encoding for Password *(p.631)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-326: Inadequate Encryption Strength *(p.796)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
- CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1250)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
- CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1340)*

CWE-730: OWASP Top Ten 2004 Category A9 - Denial of Service *(p.2339)*
- CWE-170: Improper Null Termination *(p.428)*
- CWE-248: Uncaught Exception *(p.596)*

- CWE-369: Divide By Zero *(p.913)*
- CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
- CWE-410: Insufficient Resource Pool *(p.998)*
- CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-674: Uncontrolled Recursion *(p.1484)*

CWE-731: OWASP Top Ten 2004 Category A10 - Insecure Configuration Management *(p.2339)*

- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
- CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
- CWE-275: Permission Issues *(p.2317)*
- CWE-295: Improper Certificate Validation *(p.714)*
- CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
- CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1270)*
- 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.1099)*
- CWE-489: Active Debug Code *(p.1171)*
- 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.1222)*
- CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework *(p.1269)*
- CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1271)*
- CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1234)*
- CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1236)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
- CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1238)*
- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1239)*
- CWE-531: Inclusion of Sensitive Information in Test Code *(p.1240)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
- CWE-540: Inclusion of Sensitive Information in Source Code *(p.1251)*
- CWE-541: Inclusion of Sensitive Information in an Include File *(p.1253)*
- CWE-548: Exposure of Information Through Directory Listing *(p.1261)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*

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.2340)*
  - CWE-684: Incorrect Provision of Specified Functionality *(p.1505)*
- CWE-736: CERT C Secure Coding Standard (2008) Chapter 3 - Declarations and Initialization (DCL) *(p.2341)*
  - CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1259)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
- CWE-737: CERT C Secure Coding Standard (2008) Chapter 4 - Expressions (EXP) *(p.2341)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
  - CWE-468: Incorrect Pointer Scaling *(p.1114)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-783: Operator Precedence Logic Error *(p.1650)*
- CWE-738: CERT C Secure Coding Standard (2008) Chapter 5 - Integers (INT) *(p.2342)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-192: Integer Coercion Error *(p.482)*
  - CWE-197: Numeric Truncation Error *(p.500)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1109)*
  - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*
  - CWE-606: Unchecked Input for Loop Condition *(p.1357)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1489)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-682: Incorrect Calculation *(p.1499)*
- CWE-739: CERT C Secure Coding Standard (2008) Chapter 6 - Floating Point (FLP) *(p.2343)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
- CWE-740: CERT C Secure Coding Standard (2008) Chapter 7 - Arrays (ARR) *(p.2344)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
  - CWE-469: Use of Pointer Subtraction to Determine Size *(p.1115)*
  - CWE-665: Improper Initialization *(p.1456)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
- CWE-741: CERT C Secure Coding Standard (2008) Chapter 8 - Characters and Strings (STR) *(p.2344)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.370)*
  - CWE-170: Improper Null Termination *(p.428)*
  - CWE-193: Off-by-one Error *(p.486)*
  - CWE-464: Addition of Data Structure Sentinel *(p.1107)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
- CWE-742: CERT C Secure Coding Standard (2008) Chapter 9 - Memory Management (MEM) *(p.2345)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-128: Wrap-around Error *(p.339)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-415: Double Free *(p.1008)*
- CWE-416: Use After Free *(p.1012)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
- CWE-590: Free of Memory not on the Heap *(p.1326)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
- CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
- CWE-665: Improper Initialization *(p.1456)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1510)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*

CWE-743: CERT C Secure Coding Standard (2008) Chapter 10 - Input Output (FIO) *(p.2347)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-276: Incorrect Default Permissions *(p.665)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
- CWE-37: Path Traversal: '/absolute/pathname/here' *(p.79)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.930)*
- CWE-38: Path Traversal: '\absolute\pathname\here' *(p.80)*
- CWE-39: Path Traversal: 'C:dirname' *(p.82)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-41: Improper Resolution of Path Equivalence *(p.86)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
- CWE-62: UNIX Hard Link *(p.119)*
- CWE-64: Windows Shortcut Following (.LNK) *(p.121)*
- CWE-65: Windows Hard Link *(p.123)*
- CWE-67: Improper Handling of Windows Device Names *(p.126)*
- CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1487)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*

CWE-744: CERT C Secure Coding Standard (2008) Chapter 11 - Environment (ENV) *(p.2348)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-462: Duplicate Key in Associative List (Alist) *(p.1104)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*

- CWE-745: CERT C Secure Coding Standard (2008) Chapter 12 - Signals (SIG) *(p.2349)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
  - CWE-662: Improper Synchronization *(p.1448)*
- CWE-746: CERT C Secure Coding Standard (2008) Chapter 13 - Error Handling (ERR) *(p.2350)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-544: Missing Standardized Error Handling Mechanism *(p.1256)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1489)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1542)*
- CWE-747: CERT C Secure Coding Standard (2008) Chapter 14 - Miscellaneous (MSC) *(p.2350)*
  - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
  - CWE-176: Improper Handling of Unicode Encoding *(p.440)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
  - CWE-482: Comparing instead of Assigning *(p.1157)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-563: Assignment to Variable without Use *(p.1280)*
  - CWE-570: Expression is Always False *(p.1292)*
  - CWE-571: Expression is Always True *(p.1295)*
  - CWE-697: Incorrect Comparison *(p.1530)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
- CWE-748: CERT C Secure Coding Standard (2008) Appendix - POSIX (POS) *(p.2351)*
  - CWE-170: Improper Null Termination *(p.428)*
  - CWE-242: Use of Inherently Dangerous Function *(p.586)*
  - CWE-272: Least Privilege Violation *(p.656)*
  - CWE-273: Improper Check for Dropped Privileges *(p.660)*
  - CWE-363: Race Condition Enabling Link Following *(p.897)*
  - CWE-366: Race Condition within a Thread *(p.904)*
  - CWE-562: Return of Stack Variable Address *(p.1278)*
  - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
  - CWE-667: Improper Locking *(p.1464)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
  - CWE-696: Incorrect Behavior Order *(p.1527)*

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.2352)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.281)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-752: 2009 Top 25 - Risky Resource Management *(p.2353)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-404: Improper Resource Shutdown or Release *(p.980)*
  - CWE-426: Untrusted Search Path *(p.1028)*
  - CWE-494: Download of Code Without Integrity Check *(p.1185)*
  - CWE-642: External Control of Critical State Data *(p.1414)*
  - CWE-665: Improper Initialization *(p.1456)*
  - CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-73: External Control of File Name or Path *(p.132)*
  - CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-753: 2009 Top 25 - Porous Defenses *(p.2353)*
  - CWE-250: Execution with Unnecessary Privileges *(p.599)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*

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.2355)*
  - CWE-134: Use of Externally-Controlled Format String *(p.365)*
  - CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-416: Use After Free *(p.1012)*
  - CWE-426: Untrusted Search Path *(p.1028)*
  - CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1085)*
  - CWE-456: Missing Initialization of a Variable *(p.1089)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
  - CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-749: Exposed Dangerous Method or Function *(p.1564)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-799: Improper Control of Interaction Frequency *(p.1699)*
  - CWE-804: Guessable CAPTCHA *(p.1701)*
- CWE-803: 2010 Top 25 - Porous Defenses *(p.2355)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
  - CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
- CWE-802: 2010 Top 25 - Risky Resource Management *(p.2354)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-494: Download of Code Without Integrity Check *(p.1185)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
  - CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*
- CWE-801: 2010 Top 25 - Insecure Interaction Between Components *(p.2354)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*

Graph View: CWE-809: Weaknesses in OWASP Top Ten (2010)

- CWE-810: OWASP Top Ten 2010 Category A1 - Injection *(p.2356)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-811: OWASP Top Ten 2010 Category A2 - Cross-Site Scripting (XSS) *(p.2357)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-812: OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management *(p.2357)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-813: OWASP Top Ten 2010 Category A4 - Insecure Direct Object References *(p.2357)*
  - 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.1048)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
  - CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
  - CWE-862: Missing Authorization *(p.1780)*
  - CWE-863: Incorrect Authorization *(p.1787)*
  - CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-814: OWASP Top Ten 2010 Category A5 - Cross-Site Request Forgery(CSRF) *(p.2358)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-815: OWASP Top Ten 2010 Category A6 - Security Misconfiguration *(p.2358)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
  - CWE-250: Execution with Unnecessary Privileges *(p.599)*
  - CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
  - CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-816: OWASP Top Ten 2010 Category A7 - Insecure Cryptographic Storage *(p.2359)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
- CWE-817: OWASP Top Ten 2010 Category A8 - Failure to Restrict URL Access *(p.2359)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-862: Missing Authorization *(p.1780)*
  - CWE-863: Incorrect Authorization *(p.1787)*
- CWE-818: OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection *(p.2359)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-819: OWASP Top Ten 2010 Category A10 - Unvalidated Redirects and Forwards *(p.2360)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*

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.2362)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.281)*
  - CWE-134: Use of Externally-Controlled Format String *(p.365)*
  - CWE-144: Improper Neutralization of Line Delimiters *(p.383)*
  - CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences *(p.394)*
  - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
  - CWE-182: Collapse of Data into Unsafe Value *(p.455)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.703)*
  - CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.996)*
  - CWE-625: Permissive Regular Expression *(p.1392)*
  - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1426)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-838: Inappropriate Encoding for Output Context *(p.1764)*
- CWE-846: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 3 - Declarations and Initialization (DCL) *(p.2362)*
  - CWE-665: Improper Initialization *(p.1456)*
- CWE-847: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 4 - Expressions (EXP) *(p.2363)*
  - CWE-252: Unchecked Return Value *(p.606)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
  - CWE-595: Comparison of Object References Instead of Object Contents *(p.1334)*
  - CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
- CWE-848: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 5 - Numeric Types and Operations (NUM) *(p.2363)*
  - CWE-197: Numeric Truncation Error *(p.500)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
- CWE-849: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 6 - Object Orientation (OBJ) *(p.2364)*
  - CWE-374: Passing Mutable Objects to an Untrusted Method *(p.920)*
  - CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
  - CWE-486: Comparison of Classes by Name *(p.1164)*
  - CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1174)*
  - CWE-492: Use of Inner Class Containing Sensitive Data *(p.1175)*
  - CWE-493: Critical Public Variable Without Final Modifier *(p.1182)*
  - CWE-498: Cloneable Class Containing Sensitive Information *(p.1196)*
  - CWE-500: Public Static Field Not Marked Final *(p.1200)*
  - CWE-582: Array Declared Public, Final, and Static *(p.1314)*
  - CWE-766: Critical Data Element Declared Public *(p.1607)*
- CWE-850: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 7 - Methods (MET) *(p.2364)*
  - CWE-487: Reliance on Package-level Scope *(p.1167)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1290)*
  - CWE-573: Improper Following of Specification by Caller *(p.1298)*
  - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*
  - CWE-583: finalize() Method Declared Public *(p.1315)*
  - CWE-586: Explicit Call to Finalize() *(p.1320)*
  - CWE-589: Call to Non-ubiquitous API *(p.1325)*
  - CWE-617: Reachable Assertion *(p.1378)*
- CWE-851: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 8 - Exceptional Behavior (ERR) *(p.2365)*

- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-230: Improper Handling of Missing Values *(p.570)*
- CWE-232: Improper Handling of Undefined Values *(p.573)*
- CWE-248: Uncaught Exception *(p.596)*
- CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
- CWE-390: Detection of Error Condition Without Action *(p.943)*
- CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.957)*
- CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
- CWE-584: Return Inside Finally Block *(p.1317)*
- CWE-600: Uncaught Exception in Servlet *(p.1343)*
- CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1514)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*

CWE-852: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 9 - Visibility and Atomicity (VNA) *(p.2366)*

- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-366: Race Condition within a Thread *(p.904)*
- CWE-413: Improper Resource Locking *(p.1003)*
- CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
- CWE-662: Improper Synchronization *(p.1448)*
- CWE-667: Improper Locking *(p.1464)*

CWE-853: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 10 - Locking (LCK) *(p.2366)*

- CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
- CWE-413: Improper Resource Locking *(p.1003)*
- CWE-609: Double-Checked Locking *(p.1362)*
- CWE-667: Improper Locking *(p.1464)*
- CWE-820: Missing Synchronization *(p.1720)*
- CWE-833: Deadlock *(p.1753)*

CWE-854: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 11 - Thread APIs (THI) *(p.2367)*

- CWE-572: Call to Thread run() instead of start() *(p.1296)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*

CWE-855: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 12 - Thread Pools (TPS) *(p.2367)*

- CWE-392: Missing Report of Error Condition *(p.951)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
- CWE-410: Insufficient Resource Pool *(p.998)*

CWE-856: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 13 - Thread-Safety Miscellaneous (TSM) *(p.2367)*

CWE-857: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 14 - Input Output (FIO) *(p.2368)*

- CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.370)*
- CWE-198: Use of Incorrect Byte Ordering *(p.503)*
- CWE-276: Incorrect Default Permissions *(p.665)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
- CWE-377: Insecure Temporary File *(p.925)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
- CWE-459: Incomplete Cleanup *(p.1099)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
- CWE-67: Improper Handling of Windows Device Names *(p.126)*

- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*

CWE-858: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 15 - Serialization (SER) *(p.2368)*

- CWE-250: Execution with Unnecessary Privileges *(p.599)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-499: Serializable Class Containing Sensitive Data *(p.1198)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-589: Call to Non-ubiquitous API *(p.1325)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*

CWE-859: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 16 - Platform Security (SEC) *(p.2369)*

- CWE-111: Direct Use of Unsafe JNI *(p.266)*
- CWE-266: Incorrect Privilege Assignment *(p.638)*
- CWE-272: Least Privilege Violation *(p.656)*
- CWE-300: Channel Accessible by Non-Endpoint *(p.730)*
- CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*

CWE-860: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 17 - Runtime Environment (ENV) *(p.2370)*

- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*

CWE-861: The CERT Oracle Secure Coding Standard for Java (2011) Chapter 18 - Miscellaneous (MSC) *(p.2370)*

- CWE-259: Use of Hard-coded Password *(p.623)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
- CWE-332: Insufficient Entropy in PRNG *(p.823)*
- CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.825)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*

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.2373)*
- CWE-870: CERT C++ Secure Coding Section 02 - Declarations and Initialization (DCL) *(p.2373)*
- CWE-871: CERT C++ Secure Coding Section 03 - Expressions (EXP) *(p.2374)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
  - CWE-768: Incorrect Short Circuit Evaluation *(p.1612)*
- CWE-872: CERT C++ Secure Coding Section 04 - Integers (INT) *(p.2374)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-192: Integer Coercion Error *(p.482)*
  - CWE-197: Numeric Truncation Error *(p.500)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1109)*
  - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*
  - CWE-606: Unchecked Input for Loop Condition *(p.1357)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1489)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-682: Incorrect Calculation *(p.1499)*
- CWE-873: CERT C++ Secure Coding Section 05 - Floating Point Arithmetic (FLP) *(p.2375)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
- CWE-874: CERT C++ Secure Coding Section 06 - Arrays and the STL (ARR) *(p.2375)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
  - CWE-469: Use of Pointer Subtraction to Determine Size *(p.1115)*
  - CWE-665: Improper Initialization *(p.1456)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
- CWE-875: CERT C++ Secure Coding Section 07 - Characters and Strings (STR) *(p.2376)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-170: Improper Null Termination *(p.428)*
  - CWE-193: Off-by-one Error *(p.486)*
  - CWE-464: Addition of Data Structure Sentinel *(p.1107)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
- CWE-876: CERT C++ Secure Coding Section 08 - Memory Management (MEM) *(p.2376)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-128: Wrap-around Error *(p.339)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
  - CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
  - CWE-252: Unchecked Return Value *(p.606)*

- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-415: Double Free *(p.1008)*
- CWE-416: Use After Free *(p.1012)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
- CWE-590: Free of Memory not on the Heap *(p.1326)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
- CWE-665: Improper Initialization *(p.1456)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1510)*
- CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1514)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
- CWE-762: Mismatched Memory Management Routines *(p.1596)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-822: Untrusted Pointer Dereference *(p.1723)*

CWE-877: CERT C++ Secure Coding Section 09 - Input Output (FIO) *(p.2377)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-276: Incorrect Default Permissions *(p.665)*
- CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
- CWE-37: Path Traversal: '/absolute/pathname/here' *(p.79)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.930)*
- CWE-38: Path Traversal: '\absolute\pathname\here' *(p.80)*
- CWE-39: Path Traversal: 'C:dirname' *(p.82)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-41: Improper Resolution of Path Equivalence *(p.86)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
- CWE-62: UNIX Hard Link *(p.119)*
- CWE-64: Windows Shortcut Following (.LNK) *(p.121)*
- CWE-65: Windows Hard Link *(p.123)*
- CWE-67: Improper Handling of Windows Device Names *(p.126)*
- CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1487)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-73: External Control of File Name or Path *(p.132)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*

CWE-878: CERT C++ Secure Coding Section 10 - Environment (ENV) *(p.2378)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-462: Duplicate Key in Associative List (Alist) *(p.1104)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*

- CWE-879: CERT C++ Secure Coding Section 11 - Signals (SIG) *(p.2379)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
  - CWE-662: Improper Synchronization *(p.1448)*
- CWE-880: CERT C++ Secure Coding Section 12 - Exceptions and Error Handling (ERR) *(p.2379)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-390: Detection of Error Condition Without Action *(p.943)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
  - CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
  - CWE-544: Missing Standardized Error Handling Mechanism *(p.1256)*
  - CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1542)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-755: Improper Handling of Exceptional Conditions *(p.1576)*
- CWE-881: CERT C++ Secure Coding Section 13 - Object Oriented Programming (OOP) *(p.2380)*
- CWE-882: CERT C++ Secure Coding Section 14 - Concurrency (CON) *(p.2380)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-366: Race Condition within a Thread *(p.904)*
  - CWE-404: Improper Resource Shutdown or Release *(p.980)*
  - CWE-488: Exposure of Data Element to Wrong Session *(p.1169)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-883: CERT C++ Secure Coding Section 49 - Miscellaneous (MSC) *(p.2381)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.281)*
  - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
  - CWE-176: Improper Handling of Unicode Encoding *(p.440)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
  - CWE-482: Comparing instead of Assigning *(p.1157)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-563: Assignment to Variable without Use *(p.1280)*
  - CWE-570: Expression is Always False *(p.1292)*
  - CWE-571: Expression is Always True *(p.1295)*
  - CWE-697: Incorrect Comparison *(p.1530)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*

Graph View: CWE-888: Software Fault Pattern (SFP) Clusters

- CWE-885: SFP Primary Cluster: Risky Values *(p.2382)*
  - CWE-998: SFP Secondary Cluster: Glitch in Computation *(p.2419)*
    - CWE-128: Wrap-around Error *(p.339)*
    - CWE-190: Integer Overflow or Wraparound *(p.472)*
    - CWE-191: Integer Underflow (Wrap or Wraparound) *(p.480)*
    - CWE-194: Unexpected Sign Extension *(p.491)*
    - CWE-195: Signed to Unsigned Conversion Error *(p.494)*
    - CWE-196: Unsigned to Signed Conversion Error *(p.498)*
    - CWE-197: Numeric Truncation Error *(p.500)*
    - CWE-369: Divide By Zero *(p.913)*
    - CWE-456: Missing Initialization of a Variable *(p.1089)*
    - CWE-457: Use of Uninitialized Variable *(p.1094)*
    - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1109)*
    - CWE-468: Incorrect Pointer Scaling *(p.1114)*
    - CWE-475: Undefined Behavior for Input to API *(p.1130)*
    - CWE-480: Use of Incorrect Operator *(p.1150)*
    - CWE-481: Assigning instead of Comparing *(p.1154)*
    - CWE-486: Comparison of Classes by Name *(p.1164)*
    - CWE-562: Return of Stack Variable Address *(p.1278)*
    - CWE-570: Expression is Always False *(p.1292)*
    - CWE-571: Expression is Always True *(p.1295)*
    - CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session *(p.1309)*
    - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*
    - CWE-594: J2EE Framework: Saving Unserializable Objects to Disk *(p.1332)*
    - CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
    - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
    - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
    - CWE-683: Function Call With Incorrect Order of Arguments *(p.1504)*
    - CWE-685: Function Call With Incorrect Number of Arguments *(p.1507)*
    - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
    - CWE-688: Function Call With Incorrect Variable or Reference as Argument *(p.1511)*
    - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
    - CWE-768: Incorrect Short Circuit Evaluation *(p.1612)*
- CWE-886: SFP Primary Cluster: Unused entities *(p.2382)*
  - CWE-482: Comparing instead of Assigning *(p.1157)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-563: Assignment to Variable without Use *(p.1280)*
- CWE-887: SFP Primary Cluster: API *(p.2382)*
  - CWE-1001: SFP Secondary Cluster: Use of an Improper API *(p.2420)*
    - CWE-111: Direct Use of Unsafe JNI *(p.266)*
    - CWE-227: 7PK - API Abuse *(p.2313)*
    - CWE-242: Use of Inherently Dangerous Function *(p.586)*
    - CWE-245: J2EE Bad Practices: Direct Management of Connections *(p.592)*
    - CWE-246: J2EE Bad Practices: Direct Use of Sockets *(p.594)*
    - CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
    - CWE-383: J2EE Bad Practices: Direct Use of Threads *(p.935)*
    - CWE-432: Dangerous Signal Handler not Disabled During Sensitive Operations *(p.1045)*
    - CWE-439: Behavioral Change in New Version or Environment *(p.1061)*
    - CWE-440: Expected Behavior Violation *(p.1062)*
    - CWE-474: Use of Function with Inconsistent Implementations *(p.1128)*
    - CWE-477: Use of Obsolete Function *(p.1138)*

- CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
- CWE-558: Use of getlogin() in Multithreaded Application *(p.1272)*
- CWE-572: Call to Thread run() instead of start() *(p.1296)*
- CWE-573: Improper Following of Specification by Caller *(p.1298)*
- CWE-574: EJB Bad Practices: Use of Synchronization Primitives *(p.1300)*
- CWE-575: EJB Bad Practices: Use of AWT Swing *(p.1301)*
- CWE-576: EJB Bad Practices: Use of Java I/O *(p.1304)*
- CWE-577: EJB Bad Practices: Use of Sockets *(p.1305)*
- CWE-578: EJB Bad Practices: Use of Class Loader *(p.1307)*
- CWE-586: Explicit Call to Finalize() *(p.1320)*
- CWE-589: Call to Non-ubiquitous API *(p.1325)*
- CWE-617: Reachable Assertion *(p.1378)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-684: Incorrect Provision of Specified Functionality *(p.1505)*
- CWE-695: Use of Low-Level Functionality *(p.1524)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*

CWE-889: SFP Primary Cluster: Exception Management *(p.2382)*

- CWE-960: SFP Secondary Cluster: Ambiguous Exception Type *(p.2399)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.959)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-961: SFP Secondary Cluster: Incorrect Exception Behavior *(p.2399)*
  - CWE-392: Missing Report of Error Condition *(p.951)*
  - CWE-393: Return of Wrong Status Code *(p.953)*
  - CWE-455: Non-exit on Failed Initialization *(p.1087)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
  - CWE-544: Missing Standardized Error Handling Mechanism *(p.1256)*
  - CWE-584: Return Inside Finally Block *(p.1317)*
  - CWE-636: Not Failing Securely ('Failing Open') *(p.1401)*
  - CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
- CWE-962: SFP Secondary Cluster: Unchecked Status Condition *(p.2400)*
  - CWE-248: Uncaught Exception *(p.596)*
  - CWE-252: Unchecked Return Value *(p.606)*
  - CWE-253: Incorrect Check of Function Return Value *(p.613)*
  - CWE-273: Improper Check for Dropped Privileges *(p.660)*
  - CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.672)*
  - CWE-372: Incomplete Internal State Distinction *(p.919)*
  - CWE-390: Detection of Error Condition Without Action *(p.943)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-394: Unexpected Status Code or Return Value *(p.955)*
  - CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.957)*
  - CWE-431: Missing Handler *(p.1043)*
  - CWE-478: Missing Default Case in Multiple Condition Expression *(p.1142)*
  - CWE-484: Omitted Break Statement in Switch *(p.1162)*
  - CWE-600: Uncaught Exception in Servlet *(p.1343)*
  - CWE-665: Improper Initialization *(p.1456)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-755: Improper Handling of Exceptional Conditions *(p.1576)*

CWE-890: SFP Primary Cluster: Memory Access *(p.2383)*

- CWE-970: SFP Secondary Cluster: Faulty Buffer Access *(p.2405)*
  - CWE-118: Incorrect Access of Indexable Resource ('Range Error') *(p.292)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-121: Stack-based Buffer Overflow *(p.314)*
  - CWE-122: Heap-based Buffer Overflow *(p.318)*

- CWE-123: Write-what-where Condition *(p.323)*
- CWE-124: Buffer Underwrite ('Buffer Underflow') *(p.326)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-126: Buffer Over-read *(p.334)*
- CWE-127: Buffer Under-read *(p.337)*
- CWE-129: Improper Validation of Array Index *(p.341)*
- CWE-971: SFP Secondary Cluster: Faulty Pointer Use *(p.2405)*
  - CWE-469: Use of Pointer Subtraction to Determine Size *(p.1115)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-588: Attempt to Access Child of a Non-structure Pointer *(p.1323)*
- CWE-972: SFP Secondary Cluster: Faulty String Expansion *(p.2405)*
  - CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer *(p.1656)*
- CWE-973: SFP Secondary Cluster: Improper NULL Termination *(p.2406)*
  - CWE-170: Improper Null Termination *(p.428)*
- CWE-974: SFP Secondary Cluster: Incorrect Buffer Length Computation *(p.2406)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.370)*
  - CWE-251: Often Misused: String Management *(p.2314)*
  - CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
- CWE-891: SFP Primary Cluster: Memory Management *(p.2383)*
  - CWE-969: SFP Secondary Cluster: Faulty Memory Release *(p.2404)*
    - CWE-415: Double Free *(p.1008)*
    - CWE-590: Free of Memory not on the Heap *(p.1326)*
    - CWE-761: Free of Pointer not at Start of Buffer *(p.1592)*
    - CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
- CWE-892: SFP Primary Cluster: Resource Management *(p.2383)*
  - CWE-982: SFP Secondary Cluster: Failure to Release Resource *(p.2410)*
    - CWE-404: Improper Resource Shutdown or Release *(p.980)*
    - CWE-459: Incomplete Cleanup *(p.1099)*
    - CWE-771: Missing Reference to Active Allocated Resource *(p.1622)*
    - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
    - CWE-773: Missing Reference to Active File Descriptor or Handle *(p.1629)*
    - CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
  - CWE-983: SFP Secondary Cluster: Faulty Resource Use *(p.2410)*
    - CWE-416: Use After Free *(p.1012)*
    - CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
  - CWE-984: SFP Secondary Cluster: Life Cycle *(p.2411)*
    - CWE-664: Improper Control of a Resource Through its Lifetime *(p.1454)*
    - CWE-666: Operation on Resource in Wrong Phase of Lifetime *(p.1462)*
    - CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1487)*
    - CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1523)*
  - CWE-985: SFP Secondary Cluster: Unrestricted Consumption *(p.2411)*
    - CWE-400: Uncontrolled Resource Consumption *(p.964)*
    - CWE-674: Uncontrolled Recursion *(p.1484)*
    - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
    - CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling *(p.1630)*
- CWE-893: SFP Primary Cluster: Path Resolution *(p.2384)*
  - CWE-979: SFP Secondary Cluster: Failed Chroot Jail *(p.2408)*
    - CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.589)*
  - CWE-980: SFP Secondary Cluster: Link in Resource Name Resolution *(p.2409)*
    - CWE-386: Symbolic Name not Mapping to Correct Object *(p.942)*
    - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
    - CWE-610: Externally Controlled Reference to a Resource in Another Sphere *(p.1364)*
    - CWE-62: UNIX Hard Link *(p.119)*
    - CWE-64: Windows Shortcut Following (.LNK) *(p.121)*

- CWE-65: Windows Hard Link *(p.123)*
- CWE-981: SFP Secondary Cluster: Path Traversal *(p.2409)*
  - 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.54)*
  - CWE-26: Path Traversal: '/dir/../filename' *(p.56)*
  - CWE-27: Path Traversal: 'dir/../../filename' *(p.58)*
  - CWE-28: Path Traversal: '..\filedir' *(p.59)*
  - CWE-29: Path Traversal: '\..\filename' *(p.61)*
  - CWE-30: Path Traversal: '\dir\..\filename' *(p.63)*
  - 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.80)*
  - CWE-39: Path Traversal: 'C:dirname' *(p.82)*
  - CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) *(p.85)*
  - CWE-41: Improper Resolution of Path Equivalence *(p.86)*
  - CWE-42: Path Equivalence: 'filename.' (Trailing Dot) *(p.92)*
  - CWE-428: Unquoted Search Path or Element *(p.1039)*
  - CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) *(p.93)*
  - CWE-44: Path Equivalence: 'file.name' (Internal Dot) *(p.94)*
  - CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) *(p.95)*
  - CWE-46: Path Equivalence: 'filename ' (Trailing Space) *(p.96)*
  - CWE-47: Path Equivalence: ' filename' (Leading Space) *(p.97)*
  - CWE-48: Path Equivalence: 'file name' (Internal Whitespace) *(p.98)*
  - CWE-49: Path Equivalence: 'filename/' (Trailing Slash) *(p.99)*
  - CWE-50: Path Equivalence: '//multiple/leading/slash' *(p.100)*
  - CWE-51: Path Equivalence: '/multiple//internal/slash' *(p.102)*
  - CWE-52: Path Equivalence: '/multiple/trailing/slash//' *(p.103)*
  - CWE-53: Path Equivalence: '\multiple\\internal\backslash' *(p.104)*
  - CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) *(p.105)*
  - CWE-55: Path Equivalence: '/./' (Single Dot Directory) *(p.106)*
  - CWE-56: Path Equivalence: 'filedir*' (Wildcard) *(p.107)*
  - CWE-57: Path Equivalence: 'fakedir/../realdir/filename' *(p.108)*
  - CWE-58: Path Equivalence: Windows 8.3 Filename *(p.110)*
  - CWE-66: Improper Handling of File Names that Identify Virtual Resources *(p.124)*
  - CWE-67: Improper Handling of Windows Device Names *(p.126)*
  - CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1544)*
  - CWE-72: Improper Handling of Apple HFS+ Alternate Data Stream Path *(p.130)*
  - CWE-73: External Control of File Name or Path *(p.132)*
- CWE-894: SFP Primary Cluster: Synchronization *(p.2384)*
  - CWE-986: SFP Secondary Cluster: Missing Lock *(p.2411)*
    - CWE-364: Signal Handler Race Condition *(p.899)*
    - CWE-366: Race Condition within a Thread *(p.904)*
    - CWE-368: Context Switching Race Condition *(p.912)*
    - CWE-413: Improper Resource Locking *(p.1003)*
    - CWE-414: Missing Lock Check *(p.1007)*
    - CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
    - CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*

- CWE-609: Double-Checked Locking *(p.1362)*
- CWE-662: Improper Synchronization *(p.1448)*
- CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1452)*
- CWE-667: Improper Locking *(p.1464)*

CWE-987: SFP Secondary Cluster: Multiple Locks/Unlocks *(p.2412)*
- CWE-585: Empty Synchronized Block *(p.1318)*
- CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
- CWE-765: Multiple Unlocks of a Critical Resource *(p.1605)*

CWE-988: SFP Secondary Cluster: Race Condition Window *(p.2412)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-363: Race Condition Enabling Link Following *(p.897)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
- CWE-370: Missing Check for Certificate Revocation after Initial Check *(p.917)*
- CWE-638: Not Using Complete Mediation *(p.1404)*

CWE-989: SFP Secondary Cluster: Unrestricted Lock *(p.2413)*
- CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*

CWE-895: SFP Primary Cluster: Information Leak *(p.2384)*

CWE-963: SFP Secondary Cluster: Exposed Data *(p.2400)*
- CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
- CWE-117: Improper Output Neutralization for Logs *(p.288)*
- 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.504)*
- CWE-201: Insertion of Sensitive Information Into Sent Data *(p.514)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-210: Self-generated Error Message Containing Sensitive Information *(p.539)*
- CWE-211: Externally-Generated Error Message Containing Sensitive Information *(p.541)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
- CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.547)*
- CWE-214: Invocation of Process Using Visible Sensitive Information *(p.549)*
- CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
- CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
- CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.555)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
- CWE-256: Plaintext Storage of a Password *(p.615)*
- CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
- CWE-260: Password in Configuration File *(p.629)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
- CWE-313: Cleartext Storage in a File or on Disk *(p.770)*
- CWE-314: Cleartext Storage in the Registry *(p.772)*
- CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.774)*
- CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.775)*
- CWE-317: Cleartext Storage of Sensitive Information in GUI *(p.777)*
- CWE-318: Cleartext Storage of Sensitive Information in Executable *(p.778)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-374: Passing Mutable Objects to an Untrusted Method *(p.920)*
- CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
- CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') *(p.976)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
- CWE-433: Unparsed Raw Web Content Delivery *(p.1046)*

- CWE-495: Private Data Structure Returned From A Public Method *(p.1189)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
- CWE-498: Cloneable Class Containing Sensitive Information *(p.1196)*
- CWE-499: Serializable Class Containing Sensitive Data *(p.1198)*
- CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
- CWE-501: Trust Boundary Violation *(p.1203)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-523: Unprotected Transport of Credentials *(p.1230)*
- CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1234)*
- CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1236)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
- CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1238)*
- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1239)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
- CWE-535: Exposure of Information Through Shell Error Message *(p.1244)*
- CWE-536: Servlet Runtime Error Message Containing Sensitive Information *(p.1245)*
- CWE-537: Java Runtime Error Message Containing Sensitive Information *(p.1246)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
- CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1250)*
- CWE-540: Inclusion of Sensitive Information in Source Code *(p.1251)*
- CWE-541: Inclusion of Sensitive Information in an Include File *(p.1253)*
- CWE-546: Suspicious Comment *(p.1258)*
- CWE-548: Exposure of Information Through Directory Listing *(p.1261)*
- CWE-550: Server-generated Error Message Containing Sensitive Information *(p.1263)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
- CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1270)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
- CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1340)*
- CWE-607: Public Static Final Field References Mutable Object *(p.1360)*
- CWE-612: Improper Authorization of Index Containing Sensitive Information *(p.1370)*
- CWE-615: Inclusion of Sensitive Information in Source Code Comments *(p.1375)*
- CWE-642: External Control of Critical State Data *(p.1414)*
- CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
- CWE-669: Incorrect Resource Transfer Between Spheres *(p.1471)*
- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*
- CWE-756: Missing Custom Error Page *(p.1579)*
- CWE-767: Access to Critical Private Variable via Public Method *(p.1610)*
- CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote *(p.6)*

CWE-964: SFP Secondary Cluster: Exposure Temporary File *(p.2402)*
- CWE-377: Insecure Temporary File *(p.925)*
- CWE-378: Creation of Temporary File With Insecure Permissions *(p.928)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.930)*

CWE-965: SFP Secondary Cluster: Insecure Session Management *(p.2403)*
- CWE-488: Exposure of Data Element to Wrong Session *(p.1169)*
- CWE-524: Use of Cache Containing Sensitive Information *(p.1232)*
- CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length *(p.2)*

CWE-966: SFP Secondary Cluster: Other Exposures *(p.2403)*
- CWE-453: Insecure Default Variable Initialization *(p.1083)*
- CWE-487: Reliance on Package-level Scope *(p.1167)*
- CWE-492: Use of Inner Class Containing Sensitive Data *(p.1175)*
- CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1233)*
- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute *(p.1373)*
- CWE-651: Exposure of WSDL File Containing Sensitive Information *(p.1433)*

CWE-967: SFP Secondary Cluster: State Disclosure *(p.2403)*

- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1068)*
- CWE-553: Command Shell in Externally Accessible Directory *(p.1269)*
- CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework *(p.1269)*
- CWE-564: SQL Injection: Hibernate *(p.1282)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-619: Dangling Database Cursor ('Cursor Injection') *(p.1382)*
- CWE-621: Variable Extraction Error *(p.1385)*
- CWE-624: Executable Regular Expression Error *(p.1390)*
- CWE-625: Permissive Regular Expression *(p.1392)*
- CWE-626: Null Byte Interaction Error (Poison Null Byte) *(p.1394)*
- CWE-627: Dynamic Variable Evaluation *(p.1396)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1412)*
- CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
- CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(p.1422)*
- CWE-646: Reliance on File Name or Extension of Externally-Supplied File *(p.1425)*
- CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1510)*
- CWE-707: Improper Neutralization *(p.1546)*
  - CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
  - CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) *(p.142)*
  - CWE-76: Improper Neutralization of Equivalent Special Elements *(p.144)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
  - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) *(p.177)*
  - CWE-81: Improper Neutralization of Script in an Error Message Web Page *(p.179)*
  - CWE-82: Improper Neutralization of Script in Attributes of IMG Tags in a Web Page *(p.182)*
  - CWE-83: Improper Neutralization of Script in Attributes in a Web Page *(p.183)*
  - CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page *(p.186)*
  - CWE-85: Doubled Character XSS Manipulations *(p.188)*
  - CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages *(p.190)*
  - CWE-87: Improper Neutralization of Alternate XSS Syntax *(p.192)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
  - CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
  - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
  - CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.232)*
  - CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.235)*
  - CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-991: SFP Secondary Cluster: Tainted Input to Environment *(p.2416)*
  - CWE-114: Process Control *(p.277)*

- CWE-427: Uncontrolled Search Path Element *(p.1033)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-471: Modification of Assumed-Immutable Data (MAID) *(p.1121)*
- CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
- CWE-473: PHP External Variable Modification *(p.1127)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-622: Improper Validation of Function Hook Arguments *(p.1387)*
- CWE-673: External Influence of Sphere Definition *(p.1483)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*

CWE-992: SFP Secondary Cluster: Faulty Input Transformation *(p.2416)*

- CWE-116: Improper Encoding or Escaping of Output *(p.281)*
- CWE-166: Improper Handling of Missing Special Element *(p.423)*
- CWE-167: Improper Handling of Additional Special Element *(p.425)*
- CWE-168: Improper Handling of Inconsistent Special Elements *(p.426)*
- CWE-172: Encoding Error *(p.433)*
- CWE-173: Improper Handling of Alternate Encoding *(p.435)*
- CWE-174: Double Decoding of the Same Data *(p.437)*
- CWE-175: Improper Handling of Mixed Encoding *(p.439)*
- CWE-176: Improper Handling of Unicode Encoding *(p.440)*
- CWE-177: Improper Handling of URL Encoding (Hex Encoding) *(p.442)*
- CWE-178: Improper Handling of Case Sensitivity *(p.445)*
- CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
- CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
- CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.453)*
- CWE-182: Collapse of Data into Unsafe Value *(p.455)*

CWE-993: SFP Secondary Cluster: Incorrect Input Handling *(p.2417)*

- CWE-198: Use of Incorrect Byte Ordering *(p.503)*
- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.568)*
- CWE-229: Improper Handling of Values *(p.570)*
- CWE-230: Improper Handling of Missing Values *(p.570)*
- CWE-231: Improper Handling of Extra Values *(p.572)*
- CWE-232: Improper Handling of Undefined Values *(p.573)*
- CWE-233: Improper Handling of Parameters *(p.574)*
- CWE-234: Failure to Handle Missing Parameter *(p.576)*
- CWE-235: Improper Handling of Extra Parameters *(p.578)*
- CWE-236: Improper Handling of Undefined Parameters *(p.579)*
- CWE-237: Improper Handling of Structural Elements *(p.580)*
- CWE-238: Improper Handling of Incomplete Structural Elements *(p.581)*
- CWE-239: Failure to Handle Incomplete Element *(p.582)*
- CWE-240: Improper Handling of Inconsistent Structural Elements *(p.583)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-351: Insufficient Type Distinction *(p.866)*
- CWE-354: Improper Validation of Integrity Check Value *(p.876)*

CWE-994: SFP Secondary Cluster: Tainted Input to Variable *(p.2417)*

- 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.1085)*
- CWE-496: Public Data Assigned to Private Array-Typed Field *(p.1192)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1286)*
- CWE-606: Unchecked Input for Loop Condition *(p.1357)*
- CWE-616: Incomplete Identification of Uploaded File Variables (PHP) *(p.1376)*

CWE-897: SFP Primary Cluster: Entry Points *(p.2385)*

- CWE-1002: SFP Secondary Cluster: Unexpected Entry Points *(p.2421)*
  - CWE-489: Active Debug Code *(p.1171)*
  - CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1174)*
  - CWE-493: Critical Public Variable Without Final Modifier *(p.1182)*
  - CWE-500: Public Static Field Not Marked Final *(p.1200)*
  - CWE-531: Inclusion of Sensitive Information in Test Code *(p.1240)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1290)*
  - CWE-580: clone() Method Without super.clone() *(p.1311)*
  - CWE-582: Array Declared Public, Final, and Static *(p.1314)*
  - CWE-583: finalize() Method Declared Public *(p.1315)*
  - CWE-608: Struts: Non-private Field in ActionForm Class *(p.1361)*
  - CWE-766: Critical Data Element Declared Public *(p.1607)*
- CWE-898: SFP Primary Cluster: Authentication *(p.2385)*
  - CWE-947: SFP Secondary Cluster: Authentication Bypass *(p.2394)*
    - CWE-287: Improper Authentication *(p.692)*
    - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
    - CWE-289: Authentication Bypass by Alternate Name *(p.703)*
    - CWE-303: Incorrect Implementation of Authentication Algorithm *(p.737)*
    - CWE-304: Missing Critical Step in Authentication *(p.738)*
    - CWE-305: Authentication Bypass by Primary Weakness *(p.740)*
    - CWE-308: Use of Single-factor Authentication *(p.752)*
    - CWE-309: Use of Password System for Primary Authentication *(p.754)*
    - CWE-603: Use of Client-Side Authentication *(p.1354)*
  - CWE-948: SFP Secondary Cluster: Digital Certificate *(p.2395)*
    - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
    - CWE-297: Improper Validation of Certificate with Host Mismatch *(p.722)*
    - CWE-298: Improper Validation of Certificate Expiration *(p.726)*
    - CWE-299: Improper Check for Certificate Revocation *(p.727)*
    - CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created *(p.1331)*
    - CWE-599: Missing Validation of OpenSSL Certificate *(p.1341)*
  - CWE-949: SFP Secondary Cluster: Faulty Endpoint Authentication *(p.2395)*
    - CWE-293: Using Referer Field for Authentication *(p.710)*
    - CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
    - CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
    - CWE-346: Origin Validation Error *(p.853)*
    - CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action *(p.863)*
    - CWE-360: Trust of System Event Data *(p.887)*
    - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
    - CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
    - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1426)*
  - CWE-950: SFP Secondary Cluster: Hardcoded Sensitive Data *(p.2396)*
    - CWE-258: Empty Password in Configuration File *(p.621)*
    - CWE-259: Use of Hard-coded Password *(p.623)*
    - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
    - CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1259)*
  - CWE-951: SFP Secondary Cluster: Insecure Authentication Policy *(p.2396)*
    - CWE-262: Not Using Password Aging *(p.633)*
    - CWE-263: Password Aging with Long Expiration *(p.636)*
    - CWE-521: Weak Password Requirements *(p.1223)*
    - CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1271)*
    - CWE-613: Insufficient Session Expiration *(p.1371)*
    - CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1423)*
  - CWE-952: SFP Secondary Cluster: Missing Authentication *(p.2396)*
    - CWE-306: Missing Authentication for Critical Function *(p.741)*

- CWE-620: Unverified Password Change *(p.1383)*
- CWE-953: SFP Secondary Cluster: Missing Endpoint Authentication *(p.2397)*
  - CWE-422: Unprotected Windows Messaging Channel ('Shatter') *(p.1022)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
- CWE-954: SFP Secondary Cluster: Multiple Binds to the Same Port *(p.2397)*
  - CWE-605: Multiple Binds to the Same Port *(p.1356)*
- CWE-955: SFP Secondary Cluster: Unrestricted Authentication *(p.2397)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
- CWE-899: SFP Primary Cluster: Access Control *(p.2386)*
  - CWE-944: SFP Secondary Cluster: Access Management *(p.2393)*
    - CWE-282: Improper Ownership Management *(p.676)*
    - CWE-283: Unverified Ownership *(p.678)*
    - CWE-284: Improper Access Control *(p.680)*
    - CWE-286: Incorrect User Management *(p.691)*
    - CWE-708: Incorrect Ownership Assignment *(p.1548)*
  - CWE-945: SFP Secondary Cluster: Insecure Resource Access *(p.2394)*
    - CWE-285: Improper Authorization *(p.684)*
    - CWE-424: Improper Protection of Alternate Path *(p.1023)*
    - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
    - CWE-650: Trusting HTTP Permission Methods on the Server Side *(p.1432)*
  - CWE-946: SFP Secondary Cluster: Insecure Resource Permissions *(p.2394)*
    - CWE-276: Incorrect Default Permissions *(p.665)*
    - CWE-277: Insecure Inherited Permissions *(p.668)*
    - CWE-278: Insecure Preserved Inherited Permissions *(p.669)*
    - CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
    - CWE-281: Improper Preservation of Permissions *(p.674)*
    - CWE-560: Use of umask() with chmod-style Argument *(p.1274)*
    - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-901: SFP Primary Cluster: Privilege *(p.2386)*
  - CWE-250: Execution with Unnecessary Privileges *(p.599)*
  - CWE-266: Incorrect Privilege Assignment *(p.638)*
  - CWE-267: Privilege Defined With Unsafe Actions *(p.641)*
  - CWE-268: Privilege Chaining *(p.644)*
  - CWE-269: Improper Privilege Management *(p.646)*
  - CWE-270: Privilege Context Switching Error *(p.651)*
  - CWE-271: Privilege Dropping / Lowering Errors *(p.653)*
  - CWE-272: Least Privilege Violation *(p.656)*
  - CWE-274: Improper Handling of Insufficient Privileges *(p.663)*
  - CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1222)*
  - CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
  - CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*
- CWE-902: SFP Primary Cluster: Channel *(p.2387)*
  - CWE-956: SFP Secondary Cluster: Channel Attack *(p.2397)*
    - CWE-290: Authentication Bypass by Spoofing *(p.705)*
    - CWE-294: Authentication Bypass by Capture-replay *(p.712)*
    - CWE-300: Channel Accessible by Non-Endpoint *(p.730)*
    - CWE-301: Reflection Attack in an Authentication Protocol *(p.733)*
    - CWE-419: Unprotected Primary Channel *(p.1017)*
    - CWE-420: Unprotected Alternate Channel *(p.1018)*
    - CWE-421: Race Condition During Access to Alternate Channel *(p.1020)*
    - CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1064)*
  - CWE-957: SFP Secondary Cluster: Protocol Error *(p.2398)*
    - CWE-353: Missing Support for Integrity Check *(p.874)*
    - CWE-435: Improper Interaction Between Multiple Correctly-Behaving Entities *(p.1055)*
    - CWE-436: Interpretation Conflict *(p.1057)*

- CWE-437: Incomplete Model of Endpoint Features *(p.1059)*
- CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') *(p.1581)*

CWE-903: SFP Primary Cluster: Cryptography *(p.2387)*
- CWE-958: SFP Secondary Cluster: Broken Cryptography *(p.2398)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-328: Use of Weak Hash *(p.806)*
  - CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
  - CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1589)*
- CWE-959: SFP Secondary Cluster: Weak Cryptography *(p.2398)*
  - CWE-261: Weak Encoding for Password *(p.631)*
  - CWE-322: Key Exchange without Entity Authentication *(p.788)*
  - CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.790)*
  - CWE-324: Use of a Key Past its Expiration Date *(p.792)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
  - CWE-329: Generation of Predictable IV with CBC Mode *(p.811)*
  - CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*

CWE-904: SFP Primary Cluster: Malware *(p.2387)*
- CWE-506: Embedded Malicious Code *(p.1210)*
- CWE-507: Trojan Horse *(p.1212)*
- CWE-508: Non-Replicating Malicious Code *(p.1213)*
- CWE-509: Replicating Malicious Code (Virus or Worm) *(p.1214)*
- CWE-510: Trapdoor *(p.1215)*
- CWE-511: Logic/Time Bomb *(p.1216)*
- CWE-512: Spyware *(p.1218)*
- CWE-69: Improper Handling of Windows ::DATA Alternate Data Stream *(p.129)*
- CWE-968: SFP Secondary Cluster: Covert Channel *(p.2404)*
  - CWE-385: Covert Timing Channel *(p.940)*
  - CWE-514: Covert Channel *(p.1218)*
  - CWE-515: Covert Storage Channel *(p.1220)*

CWE-905: SFP Primary Cluster: Predictability *(p.2388)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
- CWE-331: Insufficient Entropy *(p.821)*
- CWE-332: Insufficient Entropy in PRNG *(p.823)*
- CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.825)*
- CWE-334: Small Space of Random Values *(p.827)*
- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-339: Small Seed Space in PRNG *(p.840)*
- CWE-340: Generation of Predictable Numbers or Identifiers *(p.842)*
- CWE-341: Predictable from Observable State *(p.843)*
- CWE-342: Predictable Exact Value from Previous Values *(p.845)*
- CWE-343: Predictable Value Range from Previous Values *(p.847)*
- CWE-344: Use of Invariant Value in Dynamically Changing Context *(p.849)*

CWE-906: SFP Primary Cluster: UI *(p.2388)*
- CWE-995: SFP Secondary Cluster: Feature *(p.2418)*
  - CWE-447: Unimplemented or Unsupported Feature in UI *(p.1075)*
  - CWE-448: Obsolete Feature in UI *(p.1076)*
  - CWE-449: The UI Performs the Wrong Action *(p.1077)*
  - CWE-450: Multiple Interpretations of UI Input *(p.1078)*
  - CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1079)*

- CWE-549: Missing Password Field Masking *(p.1262)*
- CWE-655: Insufficient Psychological Acceptability *(p.1442)*
- CWE-996: SFP Secondary Cluster: Security *(p.2418)*
  - CWE-356: Product UI does not Warn User of Unsafe Actions *(p.879)*
  - CWE-357: Insufficient UI Warning of Dangerous Operations *(p.880)*
  - CWE-446: UI Discrepancy for Security Feature *(p.1073)*
- CWE-997: SFP Secondary Cluster: Information Loss *(p.2418)*
  - CWE-221: Information Loss or Omission *(p.556)*
  - CWE-222: Truncation of Security-relevant Information *(p.557)*
  - CWE-223: Omission of Security-relevant Information *(p.559)*
  - CWE-224: Obscured Security-relevant Information by Alternate Name *(p.561)*
- CWE-907: SFP Primary Cluster: Other *(p.2388)*
  - CWE-975: SFP Secondary Cluster: Architecture *(p.2406)*
    - CWE-348: Use of Less Trusted Source *(p.859)*
    - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
    - CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
    - CWE-637: Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism') *(p.1403)*
    - CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1430)*
    - CWE-654: Reliance on a Single Factor in a Security Decision *(p.1439)*
    - CWE-656: Reliance on Security Through Obscurity *(p.1444)*
    - CWE-657: Violation of Secure Design Principles *(p.1446)*
    - CWE-671: Lack of Administrator Control over Security *(p.1478)*
    - CWE-693: Protection Mechanism Failure *(p.1520)*
    - CWE-749: Exposed Dangerous Method or Function *(p.1564)*
  - CWE-976: SFP Secondary Cluster: Compiler *(p.2407)*
    - CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1562)*
  - CWE-977: SFP Secondary Cluster: Design *(p.2407)*
    - CWE-115: Misinterpretation of Input *(p.280)*
    - CWE-187: Partial String Comparison *(p.467)*
    - CWE-188: Reliance on Data/Memory Layout *(p.470)*
    - CWE-193: Off-by-one Error *(p.486)*
    - CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
    - CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
    - CWE-406: Insufficient Control of Network Message Volume (Network Amplification) *(p.990)*
    - CWE-407: Inefficient Algorithmic Complexity *(p.992)*
    - CWE-408: Incorrect Behavior Order: Early Amplification *(p.995)*
    - CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.996)*
    - CWE-410: Insufficient Resource Pool *(p.998)*
    - CWE-430: Deployment of Wrong Handler *(p.1042)*
    - CWE-462: Duplicate Key in Associative List (Alist) *(p.1104)*
    - CWE-463: Deletion of Data Structure Sentinel *(p.1105)*
    - CWE-464: Addition of Data Structure Sentinel *(p.1107)*
    - CWE-483: Incorrect Block Delimitation *(p.1160)*
    - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*
    - CWE-595: Comparison of Object References Instead of Object Contents *(p.1334)*
    - CWE-618: Exposed Unsafe ActiveX Method *(p.1380)*
    - CWE-648: Incorrect Use of Privileged APIs *(p.1428)*
    - CWE-670: Always-Incorrect Control Flow Implementation *(p.1475)*
    - CWE-682: Incorrect Calculation *(p.1499)*
    - CWE-691: Insufficient Control Flow Management *(p.1517)*
    - CWE-696: Incorrect Behavior Order *(p.1527)*
    - CWE-697: Incorrect Comparison *(p.1530)*
    - CWE-698: Execution After Redirect (EAR) *(p.1533)*

- CWE-705: Incorrect Control Flow Scoping *(p.1542)*
- CWE-978: SFP Secondary Cluster: Implementation *(p.2408)*
  - CWE-358: Improperly Implemented Security Check for Standard *(p.881)*
  - CWE-398: 7PK - Code Quality *(p.2323)*
  - CWE-623: Unsafe ActiveX Control Marked Safe For Scripting *(p.1389)*
  - CWE-710: Improper Adherence to Coding Standards *(p.1549)*
- CWE-1237: SFP Primary Cluster: Faulty Resource Release *(p.2482)*
  - CWE-415: Double Free *(p.1008)*
  - CWE-762: Mismatched Memory Management Routines *(p.1596)*
  - CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
- CWE-1238: SFP Primary Cluster: Failure to Release Memory *(p.2482)*
  - CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*

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.2372)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-456: Missing Initialization of a Variable *(p.1089)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
  - CWE-822: Untrusted Pointer Dereference *(p.1723)*
  - CWE-825: Expired Pointer Dereference *(p.1732)*
  - CWE-838: Inappropriate Encoding for Output Context *(p.1764)*
  - CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*
- CWE-866: 2011 Top 25 - Porous Defenses *(p.2372)*
  - CWE-250: Execution with Unnecessary Privileges *(p.599)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
  - CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
  - CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
  - CWE-862: Missing Authorization *(p.1780)*
  - CWE-863: Incorrect Authorization *(p.1787)*
- CWE-865: 2011 Top 25 - Risky Resource Management *(p.2371)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-134: Use of Externally-Controlled Format String *(p.365)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-494: Download of Code Without Integrity Check *(p.1185)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-864: 2011 Top 25 - Insecure Interaction Between Components *(p.2371)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
  - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
  - CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*

Graph View: CWE-928: Weaknesses in OWASP Top Ten (2013)

- CWE-929: OWASP Top Ten 2013 Category A1 - Injection *(p.2389)*
  - CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
    - CWE-564: SQL Injection: Hibernate *(p.1282)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
  - CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
  - CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
- CWE-930: OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management *(p.2389)*
  - CWE-256: Plaintext Storage of a Password *(p.615)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-384: Session Fixation *(p.936)*
  - CWE-522: Insufficiently Protected Credentials *(p.1225)*
  - CWE-523: Unprotected Transport of Credentials *(p.1230)*
  - CWE-613: Insufficient Session Expiration *(p.1371)*
  - CWE-620: Unverified Password Change *(p.1383)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- CWE-931: OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS) *(p.2390)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-932: OWASP Top Ten 2013 Category A4 - Insecure Direct Object References *(p.2390)*
  - 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.243)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
  - CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1544)*
- CWE-933: OWASP Top Ten 2013 Category A5 - Security Misconfiguration *(p.2391)*
  - CWE-2: 7PK - Environment *(p.2308)*
  - CWE-16: Configuration *(p.2309)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
  - CWE-548: Exposure of Information Through Directory Listing *(p.1261)*
- CWE-934: OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure *(p.2391)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
  - CWE-320: Key Management Errors *(p.2319)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-328: Use of Weak Hash *(p.806)*
- CWE-935: OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control *(p.2392)*
  - CWE-285: Improper Authorization *(p.684)*
- CWE-936: OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF) *(p.2392)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-937: OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities *(p.2392)*

- C CWE-938: OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards *(p.2393)*
  - B CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*

Graph View: CWE-1000: Research Concepts

- CWE-284: Improper Access Control *(p.680)*
  - CWE-1191: On-Chip Debug and Test Interface With Improper Access Control *(p.1980)*
  - CWE-1220: Insufficient Granularity of Access Control *(p.1992)*
    - CWE-1222: Insufficient Granularity of Address Regions Protected by Register Locks *(p.1999)*
  - CWE-1224: Improper Restriction of Write-Once Bit Fields *(p.2003)*
  - CWE-1231: Improper Prevention of Lock Bit Modification *(p.2007)*
  - CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2012)*
  - CWE-1242: Inclusion of Undocumented Features or Chicken Bits *(p.2033)*
  - CWE-1252: CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations *(p.2056)*
  - CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions *(p.2068)*
  - CWE-1259: Improper Restriction of Security Token Assignment *(p.2073)*
  - CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges *(p.2075)*
  - CWE-1262: Improper Access Control for Register Interface *(p.2081)*
  - CWE-1263: Improper Physical Access Control *(p.2085)*
    - CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug *(p.2035)*
  - CWE-1267: Policy Uses Obsolete Encoding *(p.2093)*
  - CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents *(p.2095)*
  - CWE-1270: Generation of Incorrect Security Tokens *(p.2100)*
  - CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code *(p.2108)*
  - CWE-1276: Hardware Child Block Incorrectly Connected to Parent System *(p.2113)*
  - CWE-1280: Access Control Check Implemented After Asset is Accessed *(p.2122)*
  - CWE-1283: Mutable Attestation or Measurement Reporting Data *(p.2128)*
  - CWE-1290: Incorrect Decoding of Security Identifiers *(p.2142)*
  - CWE-1292: Incorrect Conversion of Security Identifiers *(p.2147)*
  - CWE-1294: Insecure Security Identifier Mechanism *(p.2150)*
    - CWE-1302: Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC) *(p.2172)*
  - CWE-1296: Incorrect Chaining or Granularity of Debug Components *(p.2153)*
  - CWE-1304: Improperly Preserved Integrity of Hardware Configuration State During a Power Save/ Restore Operation *(p.2176)*
  - CWE-1311: Improper Translation of Security Attributes by Fabric Bridge *(p.2182)*
  - CWE-1312: Missing Protection for Mirrored Regions in On-Chip Fabric Firewall *(p.2184)*
  - CWE-1313: Hardware Allows Activation of Test or Debug Logic at Runtime *(p.2185)*
  - CWE-1315: Improper Setting of Bus Controlling Capability in Fabric End-point *(p.2190)*
  - CWE-1316: Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges *(p.2192)*
  - CWE-1317: Improper Access Control in Fabric Bridge *(p.2194)*
  - CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals *(p.2202)*
  - CWE-1323: Improper Management of Sensitive Trace Data *(p.2208)*
  - CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy *(p.2234)*
  - CWE-269: Improper Privilege Management *(p.646)*
    - CWE-250: Execution with Unnecessary Privileges *(p.599)*
    - CWE-266: Incorrect Privilege Assignment *(p.638)*
      - CWE-1022: Use of Web Link to Untrusted Target with window.opener Access *(p.1862)*
      - CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1222)*
      - CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1271)*
      - CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*
    - CWE-267: Privilege Defined With Unsafe Actions *(p.641)*
      - CWE-623: Unsafe ActiveX Control Marked Safe For Scripting *(p.1389)*
    - CWE-268: Privilege Chaining *(p.644)*
    - CWE-270: Privilege Context Switching Error *(p.651)*
    - CWE-271: Privilege Dropping / Lowering Errors *(p.653)*
      - CWE-272: Least Privilege Violation *(p.656)*

- CWE-273: Improper Check for Dropped Privileges *(p.660)*
- CWE-274: Improper Handling of Insufficient Privileges *(p.663)*
- CWE-648: Incorrect Use of Privileged APIs *(p.1428)*
- CWE-282: Improper Ownership Management *(p.676)*
  - CWE-283: Unverified Ownership *(p.678)*
  - CWE-708: Incorrect Ownership Assignment *(p.1548)*
- CWE-285: Improper Authorization *(p.684)*
  - CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2006)*
    - CWE-202: Exposure of Sensitive Information Through Data Queries *(p.516)*
    - CWE-612: Improper Authorization of Index Containing Sensitive Information *(p.1370)*
  - CWE-1256: Improper Restriction of Software Interfaces to Hardware Features *(p.2065)*
  - CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT Vendors *(p.2156)*
  - CWE-1328: Security Version Number Mutable to Older Versions *(p.2217)*
  - CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
    - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
      - CWE-433: Unparsed Raw Web Content Delivery *(p.1046)*
    - CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.555)*
    - CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1236)*
    - CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
    - CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1238)*
    - CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1239)*
    - CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1250)*
    - CWE-553: Command Shell in Externally Accessible Directory *(p.1269)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
    - CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag *(p.1854)*
    - CWE-276: Incorrect Default Permissions *(p.665)*
    - CWE-277: Insecure Inherited Permissions *(p.668)*
    - CWE-278: Insecure Preserved Inherited Permissions *(p.669)*
    - CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
    - CWE-281: Improper Preservation of Permissions *(p.674)*
    - CWE-766: Critical Data Element Declared Public *(p.1607)*
  - CWE-862: Missing Authorization *(p.1780)*
    - CWE-1314: Missing Write Protection for Parametric Data Values *(p.2187)*
    - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
    - CWE-638: Not Using Complete Mediation *(p.1404)*
      - CWE-424: Improper Protection of Alternate Path *(p.1023)*
        - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
    - CWE-939: Improper Authorization in Handler for Custom URL Scheme *(p.1840)*
  - CWE-863: Incorrect Authorization *(p.1787)*
    - CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State *(p.2037)*
    - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
    - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
      - CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1286)*
    - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1426)*
    - CWE-804: Guessable CAPTCHA *(p.1701)*
    - CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1847)*
  - CWE-926: Improper Export of Android Application Components *(p.1833)*
  - CWE-927: Use of Implicit Intent for Sensitive Communication *(p.1836)*
- CWE-286: Incorrect User Management *(p.691)*
  - CWE-842: Placement of User into Incorrect Group *(p.1775)*
- CWE-287: Improper Authentication *(p.692)*
  - CWE-1390: Weak Authentication *(p.2267)*

- CWE-1391: Use of Weak Credentials *(p.2269)*
  - CWE-1392: Use of Default Credentials *(p.2271)*
    - CWE-1393: Use of Default Password *(p.2273)*
    - CWE-1394: Use of Default Cryptographic Key *(p.2275)*
  - CWE-521: Weak Password Requirements *(p.1223)*
    - CWE-258: Empty Password in Configuration File *(p.621)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
    - CWE-259: Use of Hard-coded Password *(p.623)*
    - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-262: Not Using Password Aging *(p.633)*
- CWE-263: Password Aging with Long Expiration *(p.636)*
- CWE-289: Authentication Bypass by Alternate Name *(p.703)*
- CWE-290: Authentication Bypass by Spoofing *(p.705)*
  - CWE-291: Reliance on IP Address for Authentication *(p.708)*
  - CWE-293: Using Referer Field for Authentication *(p.710)*
  - CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action *(p.863)*
- CWE-294: Authentication Bypass by Capture-replay *(p.712)*
- CWE-301: Reflection Attack in an Authentication Protocol *(p.733)*
- CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
- CWE-303: Incorrect Implementation of Authentication Algorithm *(p.737)*
  - CWE-304: Missing Critical Step in Authentication *(p.738)*
- CWE-305: Authentication Bypass by Primary Weakness *(p.740)*
- CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
- CWE-308: Use of Single-factor Authentication *(p.752)*
- CWE-309: Use of Password System for Primary Authentication *(p.754)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
  - CWE-256: Plaintext Storage of a Password *(p.615)*
  - CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
  - CWE-260: Password in Configuration File *(p.629)*
    - CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
    - CWE-258: Empty Password in Configuration File *(p.621)*
    - CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1270)*
  - CWE-261: Weak Encoding for Password *(p.631)*
  - CWE-523: Unprotected Transport of Credentials *(p.1230)*
  - CWE-549: Missing Password Field Masking *(p.1262)*
- CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created *(p.1331)*
- CWE-603: Use of Client-Side Authentication *(p.1354)*
- CWE-620: Unverified Password Change *(p.1383)*
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- CWE-804: Guessable CAPTCHA *(p.1701)*
- CWE-836: Use of Password Hash Instead of Password for Authentication *(p.1761)*

- CWE-295: Improper Certificate Validation *(p.714)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
  - CWE-297: Improper Validation of Certificate with Host Mismatch *(p.722)*
  - CWE-298: Improper Validation of Certificate Expiration *(p.726)*
  - CWE-299: Improper Check for Certificate Revocation *(p.727)*
    - CWE-370: Missing Check for Certificate Revocation after Initial Check *(p.917)*
  - CWE-599: Missing Validation of OpenSSL Certificate *(p.1341)*
- CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
    - CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface *(p.2162)*
    - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-322: Key Exchange without Entity Authentication *(p.788)*

- CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1423)*
- CWE-346: Origin Validation Error *(p.853)*
  - CWE-1385: Missing Origin Validation in WebSockets *(p.2259)*
  - CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*
    - CWE-925: Improper Verification of Intent by Broadcast Receiver *(p.1831)*
- CWE-749: Exposed Dangerous Method or Function *(p.1564)*
  - CWE-618: Exposed Unsafe ActiveX Method *(p.1380)*
  - CWE-782: Exposed IOCTL with Insufficient Access Control *(p.1648)*
- CWE-923: Improper Restriction of Communication Channel to Intended Endpoints *(p.1827)*
  - CWE-1275: Sensitive Cookie with Improper SameSite Attribute *(p.2110)*
  - CWE-291: Reliance on IP Address for Authentication *(p.708)*
  - CWE-297: Improper Validation of Certificate with Host Mismatch *(p.722)*
  - CWE-300: Channel Accessible by Non-Endpoint *(p.730)*
  - CWE-419: Unprotected Primary Channel *(p.1017)*
  - CWE-420: Unprotected Alternate Channel *(p.1018)*
    - CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface *(p.2162)*
    - CWE-421: Race Condition During Access to Alternate Channel *(p.1020)*
    - CWE-422: Unprotected Windows Messaging Channel ('Shatter') *(p.1022)*
  - CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*
    - CWE-925: Improper Verification of Intent by Broadcast Receiver *(p.1831)*
  - CWE-941: Incorrectly Specified Destination in a Communication Channel *(p.1845)*
  - CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1847)*

CWE-435: Improper Interaction Between Multiple Correctly-Behaving Entities *(p.1055)*

- CWE-1038: Insecure Automated Optimizations *(p.1872)*
  - CWE-1037: Processor Optimization Removal or Modification of Security-critical Code *(p.1870)*
  - CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1562)*
    - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
- CWE-188: Reliance on Data/Memory Layout *(p.470)*
  - CWE-198: Use of Incorrect Byte Ordering *(p.503)*
- CWE-436: Interpretation Conflict *(p.1057)*
  - CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.271)*
  - CWE-115: Misinterpretation of Input *(p.280)*
  - CWE-437: Incomplete Model of Endpoint Features *(p.1059)*
  - CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1068)*
  - CWE-626: Null Byte Interaction Error (Poison Null Byte) *(p.1394)*
  - CWE-650: Trusting HTTP Permission Methods on the Server Side *(p.1432)*
  - CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages *(p.190)*
- CWE-439: Behavioral Change in New Version or Environment *(p.1061)*

CWE-664: Improper Control of a Resource Through its Lifetime *(p.1454)*

- CWE-118: Incorrect Access of Indexable Resource ('Range Error') *(p.292)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
    - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
      - CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer *(p.1656)*
    - CWE-125: Out-of-bounds Read *(p.330)*
      - CWE-126: Buffer Over-read *(p.334)*
      - CWE-127: Buffer Under-read *(p.337)*
    - CWE-466: Return of Pointer Value Outside of Expected Range *(p.1109)*
    - CWE-786: Access of Memory Location Before Start of Buffer *(p.1658)*
      - CWE-124: Buffer Underwrite ('Buffer Underflow') *(p.326)*
      - CWE-127: Buffer Under-read *(p.337)*
    - CWE-787: Out-of-bounds Write *(p.1661)*
      - CWE-121: Stack-based Buffer Overflow *(p.314)*
      - CWE-122: Heap-based Buffer Overflow *(p.318)*
      - CWE-123: Write-what-where Condition *(p.323)*

- CWE-124: Buffer Underwrite ('Buffer Underflow') *(p.326)*
- CWE-788: Access of Memory Location After End of Buffer *(p.1669)*
  - CWE-121: Stack-based Buffer Overflow *(p.314)*
  - CWE-122: Heap-based Buffer Overflow *(p.318)*
  - CWE-126: Buffer Over-read *(p.334)*
- CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
  - CWE-806: Buffer Access Using Size of Source Buffer *(p.1710)*
- CWE-822: Untrusted Pointer Dereference *(p.1723)*
- CWE-823: Use of Out-of-range Pointer Offset *(p.1726)*
- CWE-824: Access of Uninitialized Pointer *(p.1729)*
- CWE-825: Expired Pointer Dereference *(p.1732)*
  - CWE-415: Double Free *(p.1008)*
  - CWE-416: Use After Free *(p.1012)*

- CWE-1229: Creation of Emergent Resource *(p.2006)*
  - CWE-514: Covert Channel *(p.1218)*
    - CWE-385: Covert Timing Channel *(p.940)*
    - CWE-515: Covert Storage Channel *(p.1220)*
- CWE-1250: Improper Preservation of Consistency Between Independent Representations of Shared State *(p.2052)*
  - CWE-1249: Application-Level Admin Tool with Inconsistent View of Underlying Operating System *(p.2050)*
  - CWE-1251: Mirrored Regions with Different Values *(p.2054)*
- CWE-1329: Reliance on Component That is Not Updateable *(p.2219)*
  - CWE-1277: Firmware Not Updateable *(p.2116)*
  - CWE-1310: Missing Ability to Patch ROM Code *(p.2179)*
- CWE-221: Information Loss or Omission *(p.556)*
  - CWE-222: Truncation of Security-relevant Information *(p.557)*
  - CWE-223: Omission of Security-relevant Information *(p.559)*
    - CWE-778: Insufficient Logging *(p.1638)*
  - CWE-224: Obscured Security-relevant Information by Alternate Name *(p.561)*
  - CWE-356: Product UI does not Warn User of Unsafe Actions *(p.879)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.959)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.961)*
  - CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1079)*
    - CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User *(p.1857)*
    - CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
- CWE-372: Incomplete Internal State Distinction *(p.919)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
  - CWE-1235: Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations *(p.2017)*
  - CWE-1246: Improper Write Handling in Limited-write Non-Volatile Memories *(p.2043)*
  - CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
    - CWE-1050: Excessive Platform Resource Consumption within a Loop *(p.1885)*
    - CWE-1072: Data Resource Access without Use of Connection Pooling *(p.1912)*
    - CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses *(p.1913)*
    - CWE-1084: Invokable Control Element with Excessive File or Data Access Operations *(p.1924)*
    - CWE-1089: Large Data Table with Excessive Number of Indices *(p.1929)*
    - CWE-1094: Excessive Index Range Scan for a Data Resource *(p.1934)*
    - CWE-1176: Inefficient CPU Computation *(p.1971)*
      - CWE-1042: Static Member Data Element outside of a Singleton Class Element *(p.1876)*
      - CWE-1046: Creation of Immutable Text Using String Concatenation *(p.1881)*
      - CWE-1049: Excessive Data Query Operations in a Large Data Table *(p.1884)*
      - CWE-1063: Creation of Class Instance within a Static Code Block *(p.1901)*
      - CWE-1067: Excessive Execution of Sequential Searches of Data Resource *(p.1905)*

- CWE-406: Insufficient Control of Network Message Volume (Network Amplification) *(p.990)*
- CWE-407: Inefficient Algorithmic Complexity *(p.992)*
  - CWE-1333: Inefficient Regular Expression Complexity *(p.2230)*
- CWE-408: Incorrect Behavior Order: Early Amplification *(p.995)*
- CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.996)*
- CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
  - CWE-1325: Improperly Controlled Sequential Memory Allocation *(p.2210)*
  - CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling *(p.1630)*
  - CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
- CWE-771: Missing Reference to Active Allocated Resource *(p.1622)*
  - CWE-773: Missing Reference to Active File Descriptor or Handle *(p.1629)*
- CWE-779: Logging of Excessive Data *(p.1642)*
- CWE-920: Improper Restriction of Power Consumption *(p.1823)*

CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device *(p.2091)*
- CWE-299: Improper Check for Certificate Revocation *(p.727)*
  - CWE-370: Missing Check for Certificate Revocation after Initial Check *(p.917)*
- CWE-459: Incomplete Cleanup *(p.1099)*
  - CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
    - CWE-1239: Improper Zeroization of Hardware Register *(p.2022)*
    - CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition *(p.2104)*
    - CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component *(p.2170)*
      - CWE-1330: Remanent Data Readable after Memory Erase *(p.2222)*
    - CWE-1342: Information Exposure through Microarchitectural State after Transient Execution *(p.2250)*
    - CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1290)*
- CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
  - CWE-761: Free of Pointer not at Start of Buffer *(p.1592)*
  - CWE-762: Mismatched Memory Management Routines *(p.1596)*
    - CWE-590: Free of Memory not on the Heap *(p.1326)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-1091: Use of Object without Invoking Destructor Method *(p.1931)*
  - CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
  - CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
- CWE-410: Insufficient Resource Pool *(p.998)*
- CWE-471: Modification of Assumed-Immutable Data (MAID) *(p.1121)*
  - CWE-291: Reliance on IP Address for Authentication *(p.708)*
  - CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
  - CWE-473: PHP External Variable Modification *(p.1127)*
  - CWE-607: Public Static Final Field References Mutable Object *(p.1360)*
- CWE-487: Reliance on Package-level Scope *(p.1167)*
- CWE-495: Private Data Structure Returned From A Public Method *(p.1189)*
- CWE-496: Public Data Assigned to Private Array-Typed Field *(p.1192)*
- CWE-501: Trust Boundary Violation *(p.1203)*
- CWE-580: clone() Method Without super.clone() *(p.1311)*
- CWE-610: Externally Controlled Reference to a Resource in Another Sphere *(p.1364)*
  - CWE-15: External Control of System or Configuration Setting *(p.17)*
  - CWE-384: Session Fixation *(p.936)*
  - CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1064)*

- CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
- CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-73: External Control of File Name or Path *(p.132)*
  - CWE-114: Process Control *(p.277)*

CWE-662: Improper Synchronization *(p.1448)*
- CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
- CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1452)*
  - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
  - CWE-558: Use of getlogin() in Multithreaded Application *(p.1272)*
- CWE-667: Improper Locking *(p.1464)*
  - CWE-1232: Improper Lock Behavior After Power State Transition *(p.2010)*
  - CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2012)*
  - CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks *(p.2014)*
  - CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
  - CWE-413: Improper Resource Locking *(p.1003)*
    - CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
  - CWE-414: Missing Lock Check *(p.1007)*
  - CWE-609: Double-Checked Locking *(p.1362)*
  - CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
  - CWE-765: Multiple Unlocks of a Critical Resource *(p.1605)*
  - CWE-832: Unlock of a Resource that is not Locked *(p.1752)*
  - CWE-833: Deadlock *(p.1753)*
- CWE-820: Missing Synchronization *(p.1720)*
  - CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*
  - CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
  - CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
- CWE-821: Incorrect Synchronization *(p.1722)*
  - CWE-1088: Synchronous Access of Remote Resource without Timeout *(p.1928)*
  - CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels *(p.2086)*
  - CWE-572: Call to Thread run() instead of start() *(p.1296)*
  - CWE-574: EJB Bad Practices: Use of Synchronization Primitives *(p.1300)*

CWE-665: Improper Initialization *(p.1456)*
- CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready *(p.2120)*
- CWE-1419: Incorrect Initialization of Resource *(p.2280)*
  - CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
  - CWE-1052: Excessive Use of Hard-Coded Literals in Initialization *(p.1887)*
  - CWE-1188: Initialization of a Resource with an Insecure Default *(p.1974)*
    - CWE-453: Insecure Default Variable Initialization *(p.1083)*
  - CWE-1221: Incorrect Register Defaults or Module Parameters *(p.1996)*
  - CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1085)*
- CWE-455: Non-exit on Failed Initialization *(p.1087)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
  - CWE-1325: Improperly Controlled Sequential Memory Allocation *(p.2210)*
  - CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling *(p.1630)*
  - CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
- CWE-908: Use of Uninitialized Resource *(p.1792)*
  - CWE-457: Use of Uninitialized Variable *(p.1094)*
- CWE-909: Missing Initialization of Resource *(p.1797)*

- CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings *(p.2102)*
- CWE-456: Missing Initialization of a Variable *(p.1089)*

- CWE-666: Operation on Resource in Wrong Phase of Lifetime *(p.1462)*
  - CWE-415: Double Free *(p.1008)*
  - CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created *(p.1331)*
  - CWE-605: Multiple Binds to the Same Port *(p.1356)*
  - CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
    - CWE-298: Improper Validation of Certificate Expiration *(p.726)*
    - CWE-324: Use of a Key Past its Expiration Date *(p.792)*
    - CWE-613: Insufficient Session Expiration *(p.1371)*
    - CWE-825: Expired Pointer Dereference *(p.1732)*
      - CWE-415: Double Free *(p.1008)*
      - CWE-416: Use After Free *(p.1012)*
    - CWE-910: Use of Expired File Descriptor *(p.1800)*
  - CWE-826: Premature Release of Resource During Expected Lifetime *(p.1734)*
- CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
  - CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
    - CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
  - CWE-1282: Assumed-Immutable Data is Stored in Writable Memory *(p.2127)*
  - CWE-1327: Binding to an Unrestricted IP Address *(p.2215)*
  - CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) *(p.2225)*
  - CWE-134: Use of Externally-Controlled Format String *(p.365)*
  - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
    - CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information *(p.2071)*
    - CWE-1273: Device Unlock Credential Sharing *(p.2106)*
    - CWE-1295: Debug Messages Revealing Unnecessary Information *(p.2152)*
    - CWE-201: Insertion of Sensitive Information Into Sent Data *(p.514)*
      - CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1340)*
    - CWE-203: Observable Discrepancy *(p.518)*
      - CWE-1300: Improper Protection of Physical Side Channels *(p.2165)*
        - CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks *(p.2062)*
      - CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
      - CWE-204: Observable Response Discrepancy *(p.523)*
      - CWE-205: Observable Behavioral Discrepancy *(p.526)*
        - CWE-206: Observable Internal Behavioral Discrepancy *(p.527)*
        - CWE-207: Observable Behavioral Discrepancy With Equivalent Products *(p.528)*
      - CWE-208: Observable Timing Discrepancy *(p.529)*
        - CWE-1254: Incorrect Comparison Logic Granularity *(p.2060)*
    - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
      - CWE-210: Self-generated Error Message Containing Sensitive Information *(p.539)*
      - CWE-211: Externally-Generated Error Message Containing Sensitive Information *(p.541)*
        - CWE-535: Exposure of Information Through Shell Error Message *(p.1244)*
        - CWE-536: Servlet Runtime Error Message Containing Sensitive Information *(p.1245)*
        - CWE-537: Java Runtime Error Message Containing Sensitive Information *(p.1246)*
      - CWE-550: Server-generated Error Message Containing Sensitive Information *(p.1263)*
    - CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.547)*
    - CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
    - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
    - CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
      - CWE-214: Invocation of Process Using Visible Sensitive Information *(p.549)*

- CWE-548: Exposure of Information Through Directory Listing *(p.1261)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
  - CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
  - CWE-540: Inclusion of Sensitive Information in Source Code *(p.1251)*
    - CWE-531: Inclusion of Sensitive Information in Test Code *(p.1240)*
    - CWE-541: Inclusion of Sensitive Information in an Include File *(p.1253)*
    - CWE-615: Inclusion of Sensitive Information in Source Code Comments *(p.1375)*
  - CWE-651: Exposure of WSDL File Containing Sensitive Information *(p.1433)*
- 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.54)*
    - CWE-26: Path Traversal: '/dir/../filename' *(p.56)*
    - CWE-27: Path Traversal: 'dir/../../filename' *(p.58)*
    - CWE-28: Path Traversal: '..\filedir' *(p.59)*
    - CWE-29: Path Traversal: '\..\filename' *(p.61)*
    - CWE-30: Path Traversal: '\dir\..\filename' *(p.63)*
    - 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.80)*
    - CWE-39: Path Traversal: 'C:dirname' *(p.82)*
    - CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) *(p.85)*
- CWE-374: Passing Mutable Objects to an Untrusted Method *(p.920)*
- CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
- CWE-377: Insecure Temporary File *(p.925)*
  - CWE-378: Creation of Temporary File With Insecure Permissions *(p.928)*
  - CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.930)*
- CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') *(p.976)*
  - CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
  - CWE-619: Dangling Database Cursor ('Cursor Injection') *(p.1382)*
- CWE-427: Uncontrolled Search Path Element *(p.1033)*
- CWE-428: Unquoted Search Path or Element *(p.1039)*
- CWE-488: Exposure of Data Element to Wrong Session *(p.1169)*
- CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1174)*
- CWE-492: Use of Inner Class Containing Sensitive Data *(p.1175)*
- CWE-493: Critical Public Variable Without Final Modifier *(p.1182)*
  - CWE-500: Public Static Field Not Marked Final *(p.1200)*
- CWE-498: Cloneable Class Containing Sensitive Information *(p.1196)*
- CWE-499: Serializable Class Containing Sensitive Data *(p.1198)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
  - CWE-256: Plaintext Storage of a Password *(p.615)*
  - CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
  - CWE-260: Password in Configuration File *(p.629)*
    - CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
    - CWE-258: Empty Password in Configuration File *(p.621)*
    - CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1270)*
  - CWE-261: Weak Encoding for Password *(p.631)*
  - CWE-523: Unprotected Transport of Credentials *(p.1230)*

- CWE-549: Missing Password Field Masking *(p.1262)*
- CWE-524: Use of Cache Containing Sensitive Information *(p.1232)*
  - CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1233)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
  - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
    - CWE-433: Unparsed Raw Web Content Delivery *(p.1046)*
  - CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.555)*
  - CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1236)*
  - CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
  - CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1238)*
  - CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1239)*
  - CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1250)*
  - CWE-553: Command Shell in Externally Accessible Directory *(p.1269)*
- CWE-582: Array Declared Public, Final, and Static *(p.1314)*
- CWE-583: finalize() Method Declared Public *(p.1315)*
- CWE-608: Struts: Non-private Field in ActionForm Class *(p.1361)*
- CWE-642: External Control of Critical State Data *(p.1414)*
  - CWE-15: External Control of System or Configuration Setting *(p.17)*
  - CWE-426: Untrusted Search Path *(p.1028)*
  - CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
  - CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
    - CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision *(p.1653)*
  - CWE-73: External Control of File Name or Path *(p.132)*
    - CWE-114: Process Control *(p.277)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
  - CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag *(p.1854)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-277: Insecure Inherited Permissions *(p.668)*
  - CWE-278: Insecure Preserved Inherited Permissions *(p.669)*
  - CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
  - CWE-281: Improper Preservation of Permissions *(p.674)*
  - CWE-766: Critical Data Element Declared Public *(p.1607)*
- CWE-767: Access to Critical Private Variable via Public Method *(p.1610)*
- CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote *(p.6)*
- CWE-927: Use of Implicit Intent for Sensitive Communication *(p.1836)*

CWE-669: Incorrect Resource Transfer Between Spheres *(p.1471)*

- CWE-1420: Exposure of Sensitive Information during Transient Execution *(p.2284)*
  - CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution *(p.2290)*
  - CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution *(p.2297)*
  - CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution *(p.2302)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
  - CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information *(p.2071)*
  - CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
    - CWE-1239: Improper Zeroization of Hardware Register *(p.2022)*
    - CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition *(p.2104)*
    - CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component *(p.2170)*
      - CWE-1330: Remanent Data Readable after Memory Erase *(p.2222)*

- CWE-1342: Information Exposure through Microarchitectural State after Transient Execution *(p.2250)*
- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
- CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.589)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
  - CWE-827: Improper Control of Document Type Definition *(p.1736)*
  - CWE-830: Inclusion of Web Functionality from an Untrusted Source *(p.1747)*
  - CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*
- CWE-673: External Influence of Sphere Definition *(p.1483)*
  - CWE-426: Untrusted Search Path *(p.1028)*
- CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-1389: Incorrect Parsing of Numbers with Different Radices *(p.2263)*
  - CWE-588: Attempt to Access Child of a Non-structure Pointer *(p.1323)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
    - CWE-192: Integer Coercion Error *(p.482)*
    - CWE-194: Unexpected Sign Extension *(p.491)*
    - CWE-195: Signed to Unsigned Conversion Error *(p.494)*
    - CWE-196: Unsigned to Signed Conversion Error *(p.498)*
    - CWE-197: Numeric Truncation Error *(p.500)*
  - CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') *(p.1776)*
- CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1544)*
  - CWE-178: Improper Handling of Case Sensitivity *(p.445)*
  - 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.54)*
      - CWE-26: Path Traversal: '/dir/../filename' *(p.56)*
      - CWE-27: Path Traversal: 'dir/../../filename' *(p.58)*
      - CWE-28: Path Traversal: '..\filedir' *(p.59)*
      - CWE-29: Path Traversal: '\..\filename' *(p.61)*
      - CWE-30: Path Traversal: '\dir\..\filename' *(p.63)*
      - 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.80)*
      - CWE-39: Path Traversal: 'C:dirname' *(p.82)*
      - CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) *(p.85)*
  - CWE-386: Symbolic Name not Mapping to Correct Object *(p.942)*
  - CWE-41: Improper Resolution of Path Equivalence *(p.86)*
    - CWE-42: Path Equivalence: 'filename.' (Trailing Dot) *(p.92)*
      - CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) *(p.93)*
    - CWE-44: Path Equivalence: 'file.name' (Internal Dot) *(p.94)*
      - CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) *(p.95)*
    - CWE-46: Path Equivalence: 'filename ' (Trailing Space) *(p.96)*
    - CWE-47: Path Equivalence: ' filename' (Leading Space) *(p.97)*
    - CWE-48: Path Equivalence: 'file name' (Internal Whitespace) *(p.98)*
    - CWE-49: Path Equivalence: 'filename/' (Trailing Slash) *(p.99)*
    - CWE-50: Path Equivalence: '//multiple/leading/slash' *(p.100)*

- CWE-51: Path Equivalence: '/multiple//internal/slash' *(p.102)*
- CWE-52: Path Equivalence: '/multiple/trailing/slash//' *(p.103)*
- CWE-53: Path Equivalence: '\multiple\\internal\backslash' *(p.104)*
- CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) *(p.105)*
- CWE-55: Path Equivalence: '/./' (Single Dot Directory) *(p.106)*
- CWE-56: Path Equivalence: 'filedir*' (Wildcard) *(p.107)*
- CWE-57: Path Equivalence: 'fakedir/../realdir/filename' *(p.108)*
- CWE-58: Path Equivalence: Windows 8.3 Filename *(p.110)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
  - CWE-1386: Insecure Operation on Windows Junction / Mount Point *(p.2261)*
  - CWE-61: UNIX Symbolic Link (Symlink) Following *(p.116)*
  - CWE-62: UNIX Hard Link *(p.119)*
  - CWE-64: Windows Shortcut Following (.LNK) *(p.121)*
  - CWE-65: Windows Hard Link *(p.123)*
- CWE-66: Improper Handling of File Names that Identify Virtual Resources *(p.124)*
  - CWE-67: Improper Handling of Windows Device Names *(p.126)*
  - CWE-69: Improper Handling of Windows ::DATA Alternate Data Stream *(p.129)*
  - CWE-72: Improper Handling of Apple HFS+ Alternate Data Stream Path *(p.130)*
- CWE-827: Improper Control of Document Type Definition *(p.1736)*
- CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*

- CWE-911: Improper Update of Reference Count *(p.1801)*
- CWE-913: Improper Control of Dynamically-Managed Code Resources *(p.1805)*
  - CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
  - CWE-502: Deserialization of Untrusted Data *(p.1204)*
  - CWE-914: Improper Control of Dynamically-Identified Variables *(p.1807)*
    - CWE-621: Variable Extraction Error *(p.1385)*
    - CWE-627: Dynamic Variable Evaluation *(p.1396)*
  - CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes *(p.1809)*
    - CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') *(p.2204)*
  - CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
    - CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine *(p.2238)*
    - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
    - CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.232)*
      - CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.235)*
- CWE-922: Insecure Storage of Sensitive Information *(p.1825)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
    - CWE-313: Cleartext Storage in a File or on Disk *(p.770)*
    - CWE-314: Cleartext Storage in the Registry *(p.772)*
    - CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.774)*
    - CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.775)*
    - CWE-317: Cleartext Storage of Sensitive Information in GUI *(p.777)*
    - CWE-318: Cleartext Storage of Sensitive Information in Executable *(p.778)*
    - CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1234)*
  - CWE-921: Storage of Sensitive Data in a Mechanism without Access Control *(p.1824)*

- CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-128: Wrap-around Error *(p.339)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
    - CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
  - CWE-1335: Incorrect Bitwise Shift of Integer *(p.2235)*

- CWE-1339: Insufficient Precision or Accuracy of a Real Number *(p.2242)*
- CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.370)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-680: Integer Overflow to Buffer Overflow *(p.1493)*
- CWE-191: Integer Underflow (Wrap or Wraparound) *(p.480)*
- CWE-193: Off-by-one Error *(p.486)*
- CWE-369: Divide By Zero *(p.913)*
- CWE-468: Incorrect Pointer Scaling *(p.1114)*
- CWE-469: Use of Pointer Subtraction to Determine Size *(p.1115)*

CWE-691: Insufficient Control Flow Management *(p.1517)*
- CWE-1265: Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls *(p.2088)*
- CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready *(p.2120)*
- CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior *(p.2124)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-1223: Race Condition for Write-Once Attributes *(p.2001)*
  - CWE-1298: Hardware Logic Contains Race Conditions *(p.2158)*
  - CWE-364: Signal Handler Race Condition *(p.899)*
    - CWE-432: Dangerous Signal Handler not Disabled During Sensitive Operations *(p.1045)*
    - CWE-828: Signal Handler with Functionality that is not Asynchronous-Safe *(p.1737)*
      - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
    - CWE-831: Signal Handler Function Associated with Multiple Signals *(p.1749)*
  - CWE-366: Race Condition within a Thread *(p.904)*
  - CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
    - CWE-363: Race Condition Enabling Link Following *(p.897)*
  - CWE-368: Context Switching Race Condition *(p.912)*
  - CWE-421: Race Condition During Access to Alternate Channel *(p.1020)*
  - CWE-689: Permission Race Condition During Resource Copy *(p.1513)*
- CWE-430: Deployment of Wrong Handler *(p.1042)*
- CWE-431: Missing Handler *(p.1043)*
- CWE-662: Improper Synchronization *(p.1448)*
  - CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
  - CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1452)*
    - CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
    - CWE-558: Use of getlogin() in Multithreaded Application *(p.1272)*
  - CWE-667: Improper Locking *(p.1464)*
    - CWE-1232: Improper Lock Behavior After Power State Transition *(p.2010)*
    - CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2012)*
    - CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks *(p.2014)*
    - CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
    - CWE-413: Improper Resource Locking *(p.1003)*
      - CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
    - CWE-414: Missing Lock Check *(p.1007)*
    - CWE-609: Double-Checked Locking *(p.1362)*
    - CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
    - CWE-765: Multiple Unlocks of a Critical Resource *(p.1605)*
    - CWE-832: Unlock of a Resource that is not Locked *(p.1752)*
    - CWE-833: Deadlock *(p.1753)*
  - CWE-820: Missing Synchronization *(p.1720)*
    - CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*
    - CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
    - CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
  - CWE-821: Incorrect Synchronization *(p.1722)*

- CWE-1088: Synchronous Access of Remote Resource without Timeout *(p.1928)*
- CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels *(p.2086)*
- CWE-572: Call to Thread run() instead of start() *(p.1296)*
- CWE-574: EJB Bad Practices: Use of Synchronization Primitives *(p.1300)*

- CWE-670: Always-Incorrect Control Flow Implementation *(p.1475)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
    - CWE-481: Assigning instead of Comparing *(p.1154)*
    - CWE-482: Comparing instead of Assigning *(p.1157)*
    - CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
  - CWE-483: Incorrect Block Delimitation *(p.1160)*
  - CWE-484: Omitted Break Statement in Switch *(p.1162)*
  - CWE-617: Reachable Assertion *(p.1378)*
  - CWE-698: Execution After Redirect (EAR) *(p.1533)*
  - CWE-783: Operator Precedence Logic Error *(p.1650)*
- CWE-696: Incorrect Behavior Order *(p.1527)*
  - CWE-1190: DMA Device Enabled Too Early in Boot Phase *(p.1978)*
  - CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control *(p.1986)*
  - CWE-1280: Access Control Check Implemented After Asset is Accessed *(p.2122)*
  - CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
    - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
    - CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.453)*
  - CWE-408: Incorrect Behavior Order: Early Amplification *(p.995)*
  - CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*
  - CWE-248: Uncaught Exception *(p.596)*
    - CWE-600: Uncaught Exception in Servlet *(p.1343)*
  - CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
  - CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.957)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.959)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.961)*
  - CWE-455: Non-exit on Failed Initialization *(p.1087)*
  - CWE-584: Return Inside Finally Block *(p.1317)*
  - CWE-698: Execution After Redirect (EAR) *(p.1533)*
- CWE-768: Incorrect Short Circuit Evaluation *(p.1612)*
- CWE-799: Improper Control of Interaction Frequency *(p.1699)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-837: Improper Enforcement of a Single, Unique Action *(p.1762)*
- CWE-834: Excessive Iteration *(p.1754)*
  - CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context *(p.2207)*
  - CWE-674: Uncontrolled Recursion *(p.1484)*
    - CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*
  - CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*
- CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*

- CWE-693: Protection Mechanism Failure *(p.1520)*
  - CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations *(p.1873)*
  - CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications *(p.2049)*
  - CWE-1253: Incorrect Selection of Fuse Values *(p.2058)*
  - CWE-1269: Product Released in Non-Release Configuration *(p.2098)*
  - CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques *(p.2118)*
  - CWE-1291: Public Key Re-Use for Signing both Debug and Production Code *(p.2145)*
  - CWE-1318: Missing Support for Security Features in On-chip Fabrics or Buses *(p.2197)*

- CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) *(p.2199)*
- CWE-1326: Missing Immutable Root of Trust in Hardware *(p.2212)*
- CWE-1338: Improper Protections Against Hardware Overheating *(p.2240)*
- CWE-182: Collapse of Data into Unsafe Value *(p.455)*
- CWE-184: Incomplete List of Disallowed Inputs *(p.459)*
  - CWE-692: Incomplete Denylist to Cross-Site Scripting *(p.1519)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
    - CWE-313: Cleartext Storage in a File or on Disk *(p.770)*
    - CWE-314: Cleartext Storage in the Registry *(p.772)*
    - CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.774)*
    - CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.775)*
    - CWE-317: Cleartext Storage of Sensitive Information in GUI *(p.777)*
    - CWE-318: Cleartext Storage of Sensitive Information in Executable *(p.778)*
    - CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1234)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
    - CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
    - CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute *(p.1373)*
- CWE-326: Inadequate Encryption Strength *(p.796)*
  - CWE-328: Use of Weak Hash *(p.806)*
    - CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
      - CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
      - CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1589)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation *(p.2025)*
  - CWE-328: Use of Weak Hash *(p.806)*
    - CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
      - CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
      - CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1589)*
  - CWE-780: Use of RSA Algorithm without OAEP *(p.1644)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-1204: Generation of Weak Initialization Vector (IV) *(p.1987)*
    - CWE-329: Generation of Predictable IV with CBC Mode *(p.811)*
  - CWE-1241: Use of Predictable Algorithm in Random Number Generator *(p.2030)*
  - CWE-331: Insufficient Entropy *(p.821)*
    - CWE-332: Insufficient Entropy in PRNG *(p.823)*
    - CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.825)*
  - CWE-334: Small Space of Random Values *(p.827)*
    - CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length *(p.2)*
  - CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
    - CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
    - CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
    - CWE-339: Small Seed Space in PRNG *(p.840)*
  - CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
  - CWE-340: Generation of Predictable Numbers or Identifiers *(p.842)*
    - CWE-341: Predictable from Observable State *(p.843)*
    - CWE-342: Predictable Exact Value from Previous Values *(p.845)*
    - CWE-343: Predictable Value Range from Previous Values *(p.847)*
  - CWE-344: Use of Invariant Value in Dynamically Changing Context *(p.849)*
    - CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.790)*
    - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*
    - CWE-798: Use of Hard-coded Credentials *(p.1690)*
      - CWE-259: Use of Hard-coded Password *(p.623)*
      - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
  - CWE-1293: Missing Source Correlation of Multiple Independent Data *(p.2149)*

- CWE-346: Origin Validation Error *(p.853)*
  - CWE-1385: Missing Origin Validation in WebSockets *(p.2259)*
  - CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*
    - CWE-925: Improper Verification of Intent by Broadcast Receiver *(p.1831)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- CWE-348: Use of Less Trusted Source *(p.859)*
- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- CWE-351: Insufficient Type Distinction *(p.866)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-353: Missing Support for Integrity Check *(p.874)*
- CWE-354: Improper Validation of Integrity Check Value *(p.876)*
- CWE-360: Trust of System Event Data *(p.887)*
  - CWE-422: Unprotected Windows Messaging Channel ('Shatter') *(p.1022)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-616: Incomplete Identification of Uploaded File Variables (PHP) *(p.1376)*
- CWE-646: Reliance on File Name or Extension of Externally-Supplied File *(p.1425)*
- CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1430)*
- CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1830)*

CWE-357: Insufficient UI Warning of Dangerous Operations *(p.880)*
- CWE-450: Multiple Interpretations of UI Input *(p.1078)*

CWE-358: Improperly Implemented Security Check for Standard *(p.881)*

CWE-424: Improper Protection of Alternate Path *(p.1023)*
- CWE-425: Direct Request ('Forced Browsing') *(p.1025)*

CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
  - CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision *(p.1653)*
- CWE-603: Use of Client-Side Authentication *(p.1354)*

CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
- CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
  - CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
- CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) *(p.2225)*

CWE-654: Reliance on a Single Factor in a Security Decision *(p.1439)*
- CWE-308: Use of Single-factor Authentication *(p.752)*
- CWE-309: Use of Password System for Primary Authentication *(p.754)*

CWE-655: Insufficient Psychological Acceptability *(p.1442)*

CWE-656: Reliance on Security Through Obscurity *(p.1444)*

CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') *(p.1581)*

CWE-778: Insufficient Logging *(p.1638)*

CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
- CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
- CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action *(p.863)*
- CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision *(p.1653)*

CWE-697: Incorrect Comparison *(p.1530)*

CWE-1023: Incomplete Comparison with Missing Factors *(p.1865)*
- CWE-184: Incomplete List of Disallowed Inputs *(p.459)*
  - CWE-692: Incomplete Denylist to Cross-Site Scripting *(p.1519)*
- CWE-187: Partial String Comparison *(p.467)*
- CWE-478: Missing Default Case in Multiple Condition Expression *(p.1142)*
- CWE-839: Numeric Range Comparison Without Minimum Check *(p.1767)*

CWE-1024: Comparison of Incompatible Types *(p.1867)*

CWE-1025: Comparison Using Wrong Factors *(p.1868)*
- CWE-486: Comparison of Classes by Name *(p.1164)*
- CWE-595: Comparison of Object References Instead of Object Contents *(p.1334)*

- CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
- CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations *(p.1873)*
- CWE-1077: Floating Point Comparison with Incorrect Operator *(p.1917)*
- CWE-1254: Incorrect Comparison Logic Granularity *(p.2060)*
- CWE-183: Permissive List of Allowed Inputs *(p.458)*
  - CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1847)*
- CWE-185: Incorrect Regular Expression *(p.463)*
  - CWE-186: Overly Restrictive Regular Expression *(p.466)*
  - CWE-625: Permissive Regular Expression *(p.1392)*
    - CWE-777: Regular Expression without Anchors *(p.1636)*
- CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*

CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
- CWE-1384: Improper Handling of Physical or Environmental Conditions *(p.2257)*
  - CWE-1247: Improper Protection Against Voltage and Clock Glitches *(p.2044)*
  - CWE-1261: Improper Handling of Single Event Upsets *(p.2079)*
  - CWE-1332: Improper Handling of Faults that Lead to Instruction Skips *(p.2227)*
  - CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments *(p.2252)*
- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.568)*
  - CWE-166: Improper Handling of Missing Special Element *(p.423)*
  - CWE-167: Improper Handling of Additional Special Element *(p.425)*
  - CWE-168: Improper Handling of Inconsistent Special Elements *(p.426)*
  - CWE-229: Improper Handling of Values *(p.570)*
    - CWE-230: Improper Handling of Missing Values *(p.570)*
    - CWE-231: Improper Handling of Extra Values *(p.572)*
    - CWE-232: Improper Handling of Undefined Values *(p.573)*
  - CWE-233: Improper Handling of Parameters *(p.574)*
    - CWE-234: Failure to Handle Missing Parameter *(p.576)*
    - CWE-235: Improper Handling of Extra Parameters *(p.578)*
    - CWE-236: Improper Handling of Undefined Parameters *(p.579)*
  - CWE-237: Improper Handling of Structural Elements *(p.580)*
    - CWE-238: Improper Handling of Incomplete Structural Elements *(p.581)*
    - CWE-239: Failure to Handle Incomplete Element *(p.582)*
    - CWE-240: Improper Handling of Inconsistent Structural Elements *(p.583)*
      - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
  - CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-393: Return of Wrong Status Code *(p.953)*
- CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-252: Unchecked Return Value *(p.606)*
    - CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1514)*
  - CWE-253: Incorrect Check of Function Return Value *(p.613)*
  - CWE-273: Improper Check for Dropped Privileges *(p.660)*
  - CWE-354: Improper Validation of Integrity Check Value *(p.876)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-394: Unexpected Status Code or Return Value *(p.955)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-755: Improper Handling of Exceptional Conditions *(p.1576)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
    - CWE-210: Self-generated Error Message Containing Sensitive Information *(p.539)*
    - CWE-211: Externally-Generated Error Message Containing Sensitive Information *(p.541)*
      - CWE-535: Exposure of Information Through Shell Error Message *(p.1244)*
      - CWE-536: Servlet Runtime Error Message Containing Sensitive Information *(p.1245)*
      - CWE-537: Java Runtime Error Message Containing Sensitive Information *(p.1246)*
    - CWE-550: Server-generated Error Message Containing Sensitive Information *(p.1263)*

- CWE-42: Path Equivalence: 'filename.' (Trailing Dot) *(p.92)*
  - CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) *(p.93)*
- CWE-46: Path Equivalence: 'filename ' (Trailing Space) *(p.96)*
- CWE-49: Path Equivalence: 'filename/' (Trailing Slash) *(p.99)*
- CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) *(p.105)*
- CWE-164: Improper Neutralization of Internal Special Elements *(p.420)*
  - CWE-165: Improper Neutralization of Multiple Internal Special Elements *(p.422)*
    - CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) *(p.95)*
    - CWE-53: Path Equivalence: '\multiple\\internal\backslash' *(p.104)*
- CWE-464: Addition of Data Structure Sentinel *(p.1107)*
- CWE-790: Improper Filtering of Special Elements *(p.1678)*
  - CWE-791: Incomplete Filtering of Special Elements *(p.1680)*
    - CWE-792: Incomplete Filtering of One or More Instances of Special Elements *(p.1681)*
      - CWE-793: Only Filtering One Instance of a Special Element *(p.1683)*
      - CWE-794: Incomplete Filtering of Multiple Instances of Special Elements *(p.1684)*
    - CWE-795: Only Filtering Special Elements at a Specified Location *(p.1685)*
      - CWE-796: Only Filtering Special Elements Relative to a Marker *(p.1687)*
      - CWE-797: Only Filtering Special Elements at an Absolute Position *(p.1689)*
- CWE-170: Improper Null Termination *(p.428)*
- CWE-172: Encoding Error *(p.433)*
  - CWE-173: Improper Handling of Alternate Encoding *(p.435)*
  - CWE-174: Double Decoding of the Same Data *(p.437)*
  - CWE-175: Improper Handling of Mixed Encoding *(p.439)*
  - CWE-176: Improper Handling of Unicode Encoding *(p.440)*
  - CWE-177: Improper Handling of URL Encoding (Hex Encoding) *(p.442)*
- CWE-20: Improper Input Validation *(p.20)*
  - CWE-1173: Improper Use of Validation Framework *(p.1969)*
    - CWE-102: Struts: Duplicate Validation Forms *(p.246)*
    - CWE-105: Struts: Form Field Without Validator *(p.253)*
    - CWE-106: Struts: Plug-in Framework not in Use *(p.256)*
    - CWE-108: Struts: Unvalidated Action Form *(p.261)*
    - CWE-109: Struts: Validator Turned Off *(p.263)*
    - CWE-1174: ASP.NET Misconfiguration: Improper Model Validation *(p.1970)*
    - CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework *(p.1269)*
  - CWE-1284: Improper Validation of Specified Quantity in Input *(p.2130)*
    - CWE-606: Unchecked Input for Loop Condition *(p.1357)*
  - CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input *(p.2132)*
    - CWE-129: Improper Validation of Array Index *(p.341)*
    - CWE-781: Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code *(p.1646)*
  - CWE-1286: Improper Validation of Syntactic Correctness of Input *(p.2136)*
    - CWE-112: Missing XML Validation *(p.269)*
  - CWE-1287: Improper Validation of Specified Type of Input *(p.2138)*
  - CWE-1288: Improper Validation of Consistency within Input *(p.2139)*
  - CWE-1289: Improper Validation of Unsafe Equivalence in Input *(p.2141)*
  - CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
    - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
    - CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.453)*
  - CWE-622: Improper Validation of Function Hook Arguments *(p.1387)*
- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.568)*
  - CWE-166: Improper Handling of Missing Special Element *(p.423)*
  - CWE-167: Improper Handling of Additional Special Element *(p.425)*
  - CWE-168: Improper Handling of Inconsistent Special Elements *(p.426)*
  - CWE-229: Improper Handling of Values *(p.570)*
    - CWE-230: Improper Handling of Missing Values *(p.570)*
    - CWE-231: Improper Handling of Extra Values *(p.572)*

- CWE-232: Improper Handling of Undefined Values *(p.573)*
- CWE-233: Improper Handling of Parameters *(p.574)*
  - CWE-234: Failure to Handle Missing Parameter *(p.576)*
  - CWE-235: Improper Handling of Extra Parameters *(p.578)*
  - CWE-236: Improper Handling of Undefined Parameters *(p.579)*
- CWE-237: Improper Handling of Structural Elements *(p.580)*
  - CWE-238: Improper Handling of Incomplete Structural Elements *(p.581)*
  - CWE-239: Failure to Handle Incomplete Element *(p.582)*
  - CWE-240: Improper Handling of Inconsistent Structural Elements *(p.583)*
    - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*

- CWE-240: Improper Handling of Inconsistent Structural Elements *(p.583)*
  - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
- CWE-463: Deletion of Data Structure Sentinel *(p.1105)*
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
  - CWE-1236: Improper Neutralization of Formula Elements in a CSV File *(p.2019)*
  - CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) *(p.142)*
    - CWE-76: Improper Neutralization of Equivalent Special Elements *(p.144)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
    - CWE-624: Executable Regular Expression Error *(p.1390)*
    - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
    - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
    - CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
    - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) *(p.177)*
    - CWE-81: Improper Neutralization of Script in an Error Message Web Page *(p.179)*
    - CWE-83: Improper Neutralization of Script in Attributes in a Web Page *(p.183)*
      - CWE-82: Improper Neutralization of Script in Attributes of IMG Tags in a Web Page *(p.182)*
    - CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page *(p.186)*
    - CWE-85: Doubled Character XSS Manipulations *(p.188)*
    - CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages *(p.190)*
    - CWE-87: Improper Neutralization of Alternate XSS Syntax *(p.192)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
    - CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
    - CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
  - CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
    - CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.271)*
  - CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
    - CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine *(p.2238)*
    - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
    - CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.232)*
      - CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.235)*

- CWE-943: Improper Neutralization of Special Elements in Data Query Logic *(p.1850)*
  - CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
  - CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
    - CWE-564: SQL Injection: Hibernate *(p.1282)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
  - CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1412)*
  - CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1523)*
    - CWE-102: Struts: Duplicate Validation Forms *(p.246)*
    - CWE-462: Duplicate Key in Associative List (Alist) *(p.1104)*
  - CWE-914: Improper Control of Dynamically-Identified Variables *(p.1807)*
    - CWE-621: Variable Extraction Error *(p.1385)*
    - CWE-627: Dynamic Variable Evaluation *(p.1396)*

CWE-710: Improper Adherence to Coding Standards *(p.1549)*
- CWE-1041: Use of Redundant Code *(p.1875)*
- CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range *(p.1879)*
- CWE-1048: Invokable Control Element with Large Number of Outward Calls *(p.1883)*
- CWE-1059: Insufficient Technical Documentation *(p.1894)*
  - CWE-1053: Missing Documentation for Design *(p.1888)*
  - CWE-1110: Incomplete Design Documentation *(p.1950)*
  - CWE-1111: Incomplete I/O Documentation *(p.1951)*
  - CWE-1112: Incomplete Documentation of Program Execution *(p.1952)*
  - CWE-1118: Insufficient Documentation of Error Handling Techniques *(p.1958)*
- CWE-1061: Insufficient Encapsulation *(p.1898)*
  - CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer *(p.1889)*
  - CWE-1057: Data Access Operations Outside of Expected Data Manager Component *(p.1892)*
  - CWE-1062: Parent Class with References to Child Class *(p.1900)*
  - CWE-1083: Data Access from Outside Expected Data Manager Component *(p.1922)*
  - CWE-1090: Method Containing Access of a Member Element from Another Class *(p.1930)*
  - CWE-1100: Insufficient Isolation of System-Dependent Functions *(p.1940)*
  - CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality *(p.1945)*
    - CWE-188: Reliance on Data/Memory Layout *(p.470)*
      - CWE-198: Use of Incorrect Byte Ordering *(p.503)*
  - CWE-766: Critical Data Element Declared Public *(p.1607)*
- CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers *(p.1903)*
- CWE-1066: Missing Serialization Control Element *(p.1904)*
- CWE-1068: Inconsistency Between Implementation and Documented Design *(p.1906)*
- CWE-1076: Insufficient Adherence to Expected Conventions *(p.1916)*
  - CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor *(p.1880)*
  - CWE-1070: Serializable Data Element Containing non-Serializable Item Elements *(p.1909)*
  - CWE-1078: Inappropriate Source Code Style or Formatting *(p.1918)*
    - CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code *(p.1925)*
    - CWE-1099: Inconsistent Naming Conventions for Identifiers *(p.1939)*
    - CWE-1106: Insufficient Use of Symbolic Constants *(p.1946)*
    - CWE-1107: Insufficient Isolation of Symbolic Constant Definitions *(p.1947)*
    - CWE-1109: Use of Same Variable for Multiple Purposes *(p.1949)*
    - CWE-1113: Inappropriate Comment Style *(p.1953)*
    - CWE-1114: Inappropriate Whitespace Style *(p.1953)*
    - CWE-1115: Source Code Element without Standard Prologue *(p.1954)*

- CWE-1116: Inaccurate Comments *(p.1955)*
- CWE-1117: Callable with Insufficient Behavioral Summary *(p.1957)*
- CWE-546: Suspicious Comment *(p.1258)*
- CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1259)*
- CWE-1079: Parent Class without Virtual Destructor Method *(p.1919)*
- CWE-1082: Class Instance Self Destruction Control Element *(p.1921)*
- CWE-1087: Class with Virtual Method without a Virtual Destructor *(p.1927)*
- CWE-1091: Use of Object without Invoking Destructor Method *(p.1931)*
- CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element *(p.1937)*
- CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element *(p.1938)*
- CWE-1108: Excessive Reliance on Global Variables *(p.1948)*
- CWE-586: Explicit Call to Finalize() *(p.1320)*
- CWE-594: J2EE Framework: Saving Unserializable Objects to Disk *(p.1332)*
- CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers *(p.1932)*
- CWE-1093: Excessively Complex Data Representation *(p.1933)*
  - CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1877)*
  - CWE-1055: Multiple Inheritance from Concrete Classes *(p.1890)*
  - CWE-1074: Class with Excessively Deep Inheritance *(p.1914)*
  - CWE-1086: Class with Excessive Number of Child Classes *(p.1926)*
- CWE-1101: Reliance on Runtime Component in Generated Code *(p.1941)*
- CWE-1120: Excessive Code Complexity *(p.1960)*
  - CWE-1047: Modules with Circular Dependencies *(p.1882)*
  - CWE-1056: Invokable Control Element with Variadic Parameters *(p.1891)*
  - CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses *(p.1897)*
  - CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters *(p.1902)*
  - CWE-1075: Unconditional Control Flow Transfer outside of Switch Block *(p.1915)*
  - CWE-1080: Source Code File with Excessive Number of Lines of Code *(p.1920)*
  - CWE-1095: Loop Condition Value Update within the Loop *(p.1935)*
  - CWE-1119: Excessive Use of Unconditional Branching *(p.1959)*
  - CWE-1121: Excessive McCabe Cyclomatic Complexity *(p.1961)*
  - CWE-1122: Excessive Halstead Complexity *(p.1962)*
  - CWE-1123: Excessive Use of Self-Modifying Code *(p.1963)*
  - CWE-1124: Excessively Deep Nesting *(p.1964)*
  - CWE-1125: Excessive Attack Surface *(p.1965)*
- CWE-1126: Declaration of Variable with Unnecessarily Wide Scope *(p.1966)*
- CWE-1127: Compilation with Insufficient Warnings or Errors *(p.1966)*
- CWE-1164: Irrelevant Code *(p.1967)*
  - CWE-107: Struts: Unused Validation Form *(p.259)*
  - CWE-1071: Empty Code Block *(p.1910)*
    - CWE-1069: Empty Exception Block *(p.1907)*
    - CWE-585: Empty Synchronized Block *(p.1318)*
  - CWE-110: Struts: Validator Without Form Field *(p.264)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-563: Assignment to Variable without Use *(p.1280)*
- CWE-1177: Use of Prohibited Code *(p.1972)*
  - CWE-242: Use of Inherently Dangerous Function *(p.586)*
  - CWE-676: Use of Potentially Dangerous Function *(p.1489)*
    - CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer *(p.1656)*
- CWE-1209: Failure to Disable Reserved Bits *(p.1991)*
- CWE-1357: Reliance on Insufficiently Trustworthy Component *(p.2254)*
  - CWE-1104: Use of Unmaintained Third Party Components *(p.1944)*
  - CWE-1329: Reliance on Component That is Not Updateable *(p.2219)*

- CWE-1277: Firmware Not Updateable *(p.2116)*
- CWE-1310: Missing Ability to Patch ROM Code *(p.2179)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-477: Use of Obsolete Function *(p.1138)*
- CWE-484: Omitted Break Statement in Switch *(p.1162)*
- CWE-489: Active Debug Code *(p.1171)*
  - CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
- CWE-570: Expression is Always False *(p.1292)*
- CWE-571: Expression is Always True *(p.1295)*
- CWE-573: Improper Following of Specification by Caller *(p.1298)*
  - CWE-103: Struts: Incomplete validate() Method Definition *(p.248)*
  - CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.251)*
  - CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.589)*
  - CWE-253: Incorrect Check of Function Return Value *(p.613)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
  - CWE-304: Missing Critical Step in Authentication *(p.738)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-329: Generation of Predictable IV with CBC Mode *(p.811)*
  - CWE-358: Improperly Implemented Security Check for Standard *(p.881)*
  - CWE-475: Undefined Behavior for Input to API *(p.1130)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1290)*
  - CWE-577: EJB Bad Practices: Use of Sockets *(p.1305)*
  - CWE-578: EJB Bad Practices: Use of Class Loader *(p.1307)*
  - CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session *(p.1309)*
  - CWE-580: clone() Method Without super.clone() *(p.1311)*
  - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
    - CWE-683: Function Call With Incorrect Order of Arguments *(p.1504)*
    - CWE-685: Function Call With Incorrect Number of Arguments *(p.1507)*
    - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
    - CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1510)*
      - CWE-560: Use of umask() with chmod-style Argument *(p.1274)*
    - CWE-688: Function Call With Incorrect Variable or Reference as Argument *(p.1511)*
  - CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1487)*
    - CWE-1341: Multiple Releases of Same Resource or Handle *(p.2246)*
      - CWE-415: Double Free *(p.1008)*
    - CWE-174: Double Decoding of the Same Data *(p.437)*
    - CWE-605: Multiple Binds to the Same Port *(p.1356)*
    - CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
    - CWE-765: Multiple Unlocks of a Critical Resource *(p.1605)*
  - CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1523)*
    - CWE-102: Struts: Duplicate Validation Forms *(p.246)*
    - CWE-462: Duplicate Key in Associative List (Alist) *(p.1104)*
  - CWE-695: Use of Low-Level Functionality *(p.1524)*
    - CWE-111: Direct Use of Unsafe JNI *(p.266)*
    - CWE-245: J2EE Bad Practices: Direct Management of Connections *(p.592)*
    - CWE-246: J2EE Bad Practices: Direct Use of Sockets *(p.594)*
    - CWE-383: J2EE Bad Practices: Direct Use of Threads *(p.935)*
    - CWE-574: EJB Bad Practices: Use of Synchronization Primitives *(p.1300)*
    - CWE-575: EJB Bad Practices: Use of AWT Swing *(p.1301)*
    - CWE-576: EJB Bad Practices: Use of Java I/O *(p.1304)*
- CWE-657: Violation of Secure Design Principles *(p.1446)*
  - CWE-1192: Improper Identifier for IP Block used in System-On-Chip (SOC) *(p.1985)*
  - CWE-1395: Dependency on Vulnerable Third-Party Component *(p.2277)*
  - CWE-250: Execution with Unnecessary Privileges *(p.599)*

- CWE-636: Not Failing Securely ('Failing Open') *(p.1401)*
  - CWE-455: Non-exit on Failed Initialization *(p.1087)*
- CWE-637: Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism') *(p.1403)*
- CWE-638: Not Using Complete Mediation *(p.1404)*
  - CWE-424: Improper Protection of Alternate Path *(p.1023)*
    - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
- CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
  - CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
    - CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
  - CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) *(p.2225)*
- CWE-654: Reliance on a Single Factor in a Security Decision *(p.1439)*
  - CWE-308: Use of Single-factor Authentication *(p.752)*
  - CWE-309: Use of Password System for Primary Authentication *(p.754)*
- CWE-655: Insufficient Psychological Acceptability *(p.1442)*
- CWE-656: Reliance on Security Through Obscurity *(p.1444)*
- CWE-671: Lack of Administrator Control over Security *(p.1478)*
  - CWE-447: Unimplemented or Unsupported Feature in UI *(p.1075)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
    - CWE-259: Use of Hard-coded Password *(p.623)*
    - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*

- CWE-684: Incorrect Provision of Specified Functionality *(p.1505)*
  - CWE-1245: Improper Finite State Machines (FSMs) in Hardware Logic *(p.2041)*
  - CWE-392: Missing Report of Error Condition *(p.951)*
  - CWE-393: Return of Wrong Status Code *(p.953)*
  - CWE-440: Expected Behavior Violation *(p.1062)*
  - CWE-446: UI Discrepancy for Security Feature *(p.1073)*
    - CWE-447: Unimplemented or Unsupported Feature in UI *(p.1075)*
    - CWE-448: Obsolete Feature in UI *(p.1076)*
    - CWE-449: The UI Performs the Wrong Action *(p.1077)*
  - CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1079)*
    - CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User *(p.1857)*
    - CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
  - CWE-912: Hidden Functionality *(p.1803)*
    - CWE-506: Embedded Malicious Code *(p.1210)*
      - CWE-507: Trojan Horse *(p.1212)*
        - CWE-508: Non-Replicating Malicious Code *(p.1213)*
        - CWE-509: Replicating Malicious Code (Virus or Worm) *(p.1214)*
      - CWE-510: Trapdoor *(p.1215)*
      - CWE-511: Logic/Time Bomb *(p.1216)*
      - CWE-512: Spyware *(p.1218)*

- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
  - CWE-1038: Insecure Automated Optimizations *(p.1872)*
    - CWE-1037: Processor Optimization Removal or Modification of Security-critical Code *(p.1870)*
    - CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1562)*
      - CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
  - CWE-1102: Reliance on Machine-Dependent Data Representation *(p.1942)*
  - CWE-1103: Use of Platform-Dependent Third Party Components *(p.1943)*
  - CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality *(p.1945)*
    - CWE-188: Reliance on Data/Memory Layout *(p.470)*
      - CWE-198: Use of Incorrect Byte Ordering *(p.503)*
  - CWE-474: Use of Function with Inconsistent Implementations *(p.1128)*
    - CWE-589: Call to Non-ubiquitous API *(p.1325)*
  - CWE-562: Return of Stack Variable Address *(p.1278)*
  - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*

- CWE-588: Attempt to Access Child of a Non-structure Pointer *(p.1323)*

Graph View: CWE-1003: Weaknesses for Simplified Mapping of Published Vulnerabilities

- CWE-20: Improper Input Validation *(p.20)*
  - CWE-1284: Improper Validation of Specified Quantity in Input *(p.2130)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
  - CWE-1236: Improper Neutralization of Formula Elements in a CSV File *(p.2019)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
  - CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
  - CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-116: Improper Encoding or Escaping of Output *(p.281)*
  - CWE-838: Inappropriate Encoding for Output Context *(p.1764)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-125: Out-of-bounds Read *(p.330)*
  - CWE-787: Out-of-bounds Write *(p.1661)*
  - CWE-824: Access of Uninitialized Pointer *(p.1729)*
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
  - CWE-203: Observable Discrepancy *(p.518)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
- CWE-269: Improper Privilege Management *(p.646)*
- CWE-287: Improper Authentication *(p.692)*
  - CWE-290: Authentication Bypass by Spoofing *(p.705)*
  - CWE-294: Authentication Bypass by Capture-replay *(p.712)*
  - CWE-295: Improper Certificate Validation *(p.714)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-521: Weak Password Requirements *(p.1223)*
  - CWE-522: Insufficiently Protected Credentials *(p.1225)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-326: Inadequate Encryption Strength *(p.796)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-331: Insufficient Entropy *(p.821)*
  - CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
  - CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
  - CWE-346: Origin Validation Error *(p.853)*
  - CWE-347: Improper Verification of Cryptographic Signature *(p.857)*

- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-354: Improper Validation of Integrity Check Value *(p.876)*
- CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1830)*

CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*

CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-920: Improper Restriction of Power Consumption *(p.1823)*

CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- CWE-459: Incomplete Cleanup *(p.1099)*
- CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*

CWE-407: Inefficient Algorithmic Complexity *(p.992)*
- CWE-1333: Inefficient Regular Expression Complexity *(p.2230)*

CWE-436: Interpretation Conflict *(p.1057)*
- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1068)*

CWE-610: Externally Controlled Reference to a Resource in Another Sphere *(p.1364)*
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
- CWE-384: Session Fixation *(p.936)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*

CWE-662: Improper Synchronization *(p.1448)*
- CWE-667: Improper Locking *(p.1464)*

CWE-665: Improper Initialization *(p.1456)*
- CWE-1188: Initialization of a Resource with an Insecure Default *(p.1974)*
- CWE-908: Use of Uninitialized Resource *(p.1792)*
- CWE-909: Missing Initialization of Resource *(p.1797)*

CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-427: Uncontrolled Search Path Element *(p.1033)*
- CWE-428: Unquoted Search Path or Element *(p.1039)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*

CWE-669: Incorrect Resource Transfer Between Spheres *(p.1471)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
- CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*

CWE-670: Always-Incorrect Control Flow Implementation *(p.1475)*
- CWE-617: Reachable Assertion *(p.1378)*

CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
- CWE-415: Double Free *(p.1008)*
- CWE-416: Use After Free *(p.1012)*
- CWE-613: Insufficient Session Expiration *(p.1371)*

CWE-674: Uncontrolled Recursion *(p.1484)*
- CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*

CWE-682: Incorrect Calculation *(p.1499)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*

- CWE-191: Integer Underflow (Wrap or Wraparound) *(p.480)*
- CWE-193: Off-by-one Error *(p.486)*
- CWE-369: Divide By Zero *(p.913)*

CWE-697: Incorrect Comparison *(p.1530)*

CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') *(p.1776)*

CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1544)*
- CWE-178: Improper Handling of Case Sensitivity *(p.445)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*

CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-276: Incorrect Default Permissions *(p.665)*
- CWE-281: Improper Preservation of Permissions *(p.674)*

CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-273: Improper Check for Dropped Privileges *(p.660)*
- CWE-476: NULL Pointer Dereference *(p.1132)*

CWE-755: Improper Handling of Exceptional Conditions *(p.1576)*

CWE-834: Excessive Iteration *(p.1754)*
- CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*

CWE-862: Missing Authorization *(p.1780)*
- CWE-425: Direct Request ('Forced Browsing') *(p.1025)*

CWE-863: Incorrect Authorization *(p.1787)*
- CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*

CWE-913: Improper Control of Dynamically-Managed Code Resources *(p.1805)*
- CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') *(p.2204)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*

CWE-922: Insecure Storage of Sensitive Information *(p.1825)*

Graph View: CWE-1008: Architectural Concepts

- CWE-1009: Audit *(p.2424)*
  - CWE-117: Improper Output Neutralization for Logs *(p.288)*
  - CWE-223: Omission of Security-relevant Information *(p.559)*
  - CWE-224: Obscured Security-relevant Information by Alternate Name *(p.561)*
  - CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
  - CWE-778: Insufficient Logging *(p.1638)*
  - CWE-779: Logging of Excessive Data *(p.1642)*
- CWE-1010: Authenticate Actors *(p.2424)*
  - CWE-258: Empty Password in Configuration File *(p.621)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-262: Not Using Password Aging *(p.633)*
  - CWE-263: Password Aging with Long Expiration *(p.636)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.703)*
  - CWE-290: Authentication Bypass by Spoofing *(p.705)*
  - CWE-291: Reliance on IP Address for Authentication *(p.708)*
  - CWE-293: Using Referer Field for Authentication *(p.710)*
  - CWE-294: Authentication Bypass by Capture-replay *(p.712)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.733)*
  - CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
  - CWE-303: Incorrect Implementation of Authentication Algorithm *(p.737)*
  - CWE-304: Missing Critical Step in Authentication *(p.738)*
  - CWE-305: Authentication Bypass by Primary Weakness *(p.740)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
  - CWE-308: Use of Single-factor Authentication *(p.752)*
  - CWE-322: Key Exchange without Entity Authentication *(p.788)*
  - CWE-521: Weak Password Requirements *(p.1223)*
  - CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created *(p.1331)*
  - CWE-603: Use of Client-Side Authentication *(p.1354)*
  - CWE-620: Unverified Password Change *(p.1383)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
  - CWE-798: Use of Hard-coded Credentials *(p.1690)*
  - CWE-836: Use of Password Hash Instead of Password for Authentication *(p.1761)*
  - CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
- CWE-1011: Authorize Actors *(p.2425)*
  - CWE-114: Process Control *(p.277)*
  - CWE-15: External Control of System or Configuration Setting *(p.17)*
  - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
  - CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.555)*
  - CWE-266: Incorrect Privilege Assignment *(p.638)*
  - CWE-267: Privilege Defined With Unsafe Actions *(p.641)*
  - CWE-268: Privilege Chaining *(p.644)*
  - CWE-269: Improper Privilege Management *(p.646)*
  - CWE-270: Privilege Context Switching Error *(p.651)*
  - CWE-271: Privilege Dropping / Lowering Errors *(p.653)*
  - CWE-272: Least Privilege Violation *(p.656)*
  - CWE-273: Improper Check for Dropped Privileges *(p.660)*
  - CWE-274: Improper Handling of Insufficient Privileges *(p.663)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-277: Insecure Inherited Permissions *(p.668)*

- CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
- CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.672)*
- CWE-281: Improper Preservation of Permissions *(p.674)*
- CWE-282: Improper Ownership Management *(p.676)*
- CWE-283: Unverified Ownership *(p.678)*
- CWE-284: Improper Access Control *(p.680)*
- CWE-285: Improper Authorization *(p.684)*
- CWE-286: Incorrect User Management *(p.691)*
- CWE-300: Channel Accessible by Non-Endpoint *(p.730)*
- CWE-341: Predictable from Observable State *(p.843)*
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
- CWE-419: Unprotected Primary Channel *(p.1017)*
- CWE-420: Unprotected Alternate Channel *(p.1018)*
- CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1236)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
- CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1238)*
- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1239)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
- CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
- CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1286)*
- CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
- CWE-642: External Control of Critical State Data *(p.1414)*
- CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1426)*
- CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
- CWE-656: Reliance on Security Through Obscurity *(p.1444)*
- CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
- CWE-669: Incorrect Resource Transfer Between Spheres *(p.1471)*
- CWE-671: Lack of Administrator Control over Security *(p.1478)*
- CWE-673: External Influence of Sphere Definition *(p.1483)*
- CWE-708: Incorrect Ownership Assignment *(p.1548)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-782: Exposed IOCTL with Insufficient Access Control *(p.1648)*
- CWE-827: Improper Control of Document Type Definition *(p.1736)*
- CWE-862: Missing Authorization *(p.1780)*
- CWE-863: Incorrect Authorization *(p.1787)*
- CWE-921: Storage of Sensitive Data in a Mechanism without Access Control *(p.1824)*
- CWE-923: Improper Restriction of Communication Channel to Intended Endpoints *(p.1827)*
- CWE-939: Improper Authorization in Handler for Custom URL Scheme *(p.1840)*
- CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1847)*

CWE-1012: Cross Cutting *(p.2427)*

- CWE-208: Observable Timing Discrepancy *(p.529)*
- CWE-392: Missing Report of Error Condition *(p.951)*
- CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
- CWE-544: Missing Standardized Error Handling Mechanism *(p.1256)*
- CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*

- CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision *(p.1653)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*

CWE-1013: Encrypt Data *(p.2428)*

- CWE-256: Plaintext Storage of a Password *(p.615)*
- CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
- CWE-260: Password in Configuration File *(p.629)*
- CWE-261: Weak Encoding for Password *(p.631)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
- CWE-313: Cleartext Storage in a File or on Disk *(p.770)*
- CWE-314: Cleartext Storage in the Registry *(p.772)*
- CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.774)*
- CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.775)*
- CWE-317: Cleartext Storage of Sensitive Information in GUI *(p.777)*
- CWE-318: Cleartext Storage of Sensitive Information in Executable *(p.778)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.790)*
- CWE-324: Use of a Key Past its Expiration Date *(p.792)*
- CWE-325: Missing Cryptographic Step *(p.794)*
- CWE-326: Inadequate Encryption Strength *(p.796)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
- CWE-328: Use of Weak Hash *(p.806)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
- CWE-331: Insufficient Entropy *(p.821)*
- CWE-332: Insufficient Entropy in PRNG *(p.823)*
- CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.825)*
- CWE-334: Small Space of Random Values *(p.827)*
- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-339: Small Seed Space in PRNG *(p.840)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-523: Unprotected Transport of Credentials *(p.1230)*
- CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') *(p.1581)*
- CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
- CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1589)*
- CWE-780: Use of RSA Algorithm without OAEP *(p.1644)*
- CWE-922: Insecure Storage of Sensitive Information *(p.1825)*

CWE-1014: Identify Actors *(p.2429)*

- CWE-295: Improper Certificate Validation *(p.714)*
- CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
- CWE-297: Improper Validation of Certificate with Host Mismatch *(p.722)*
- CWE-298: Improper Validation of Certificate Expiration *(p.726)*
- CWE-299: Improper Check for Certificate Revocation *(p.727)*
- CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
- CWE-346: Origin Validation Error *(p.853)*
- CWE-370: Missing Check for Certificate Revocation after Initial Check *(p.917)*
- CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1064)*
- CWE-599: Missing Validation of OpenSSL Certificate *(p.1341)*
- CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*

- CWE-795: Only Filtering Special Elements at a Specified Location *(p.1685)*
- CWE-796: Only Filtering Special Elements Relative to a Marker *(p.1687)*
- CWE-797: Only Filtering Special Elements at an Absolute Position *(p.1689)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-943: Improper Neutralization of Special Elements in Data Query Logic *(p.1850)*
- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
- CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.232)*
- CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.235)*
- CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*

CWE-1020: Verify Message Integrity *(p.2434)*

- CWE-353: Missing Support for Integrity Check *(p.874)*
- CWE-354: Improper Validation of Integrity Check Value *(p.876)*
- CWE-390: Detection of Error Condition Without Action *(p.943)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
- CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1430)*
- CWE-707: Improper Neutralization *(p.1546)*
- CWE-755: Improper Handling of Exceptional Conditions *(p.1576)*
- CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1830)*

Graph View: CWE-1026: Weaknesses in OWASP Top Ten (2017)

- CWE-1027: OWASP Top Ten 2017 Category A1 - Injection *(p.2435)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
  - CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
  - CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
  - CWE-564: SQL Injection: Hibernate *(p.1282)*
  - CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
  - CWE-943: Improper Neutralization of Special Elements in Data Query Logic *(p.1850)*
- CWE-1028: OWASP Top Ten 2017 Category A2 - Broken Authentication *(p.2436)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-256: Plaintext Storage of a Password *(p.615)*
  - CWE-308: Use of Single-factor Authentication *(p.752)*
  - CWE-384: Session Fixation *(p.936)*
  - CWE-522: Insufficiently Protected Credentials *(p.1225)*
  - CWE-523: Unprotected Transport of Credentials *(p.1230)*
  - CWE-613: Insufficient Session Expiration *(p.1371)*
  - CWE-620: Unverified Password Change *(p.1383)*
  - CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- CWE-1029: OWASP Top Ten 2017 Category A3 - Sensitive Data Exposure *(p.2436)*
  - CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.555)*
  - CWE-295: Improper Certificate Validation *(p.714)*
  - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
  - CWE-320: Key Management Errors *(p.2319)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-328: Use of Weak Hash *(p.806)*
  - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
- CWE-1030: OWASP Top Ten 2017 Category A4 - XML External Entities (XXE) *(p.2437)*
  - CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
  - CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*
- CWE-1031: OWASP Top Ten 2017 Category A5 - Broken Access Control *(p.2437)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-284: Improper Access Control *(p.680)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
- CWE-1032: OWASP Top Ten 2017 Category A6 - Security Misconfiguration *(p.2438)*
  - CWE-16: Configuration *(p.2309)*
  - CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
  - CWE-548: Exposure of Information Through Directory Listing *(p.1261)*
- CWE-1033: OWASP Top Ten 2017 Category A7 - Cross-Site Scripting (XSS) *(p.2438)*
  - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*

- CWE-1034: OWASP Top Ten 2017 Category A8 - Insecure Deserialization *(p.2438)*
  - CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-1035: OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities *(p.2439)*
- CWE-1036: OWASP Top Ten 2017 Category A10 - Insufficient Logging & Monitoring *(p.2439)*
  - CWE-223: Omission of Security-relevant Information *(p.559)*
  - CWE-778: Insufficient Logging *(p.1638)*

Graph View: CWE-1128: CISQ Quality Measures (2016)

- CWE-1129: CISQ Quality Measures (2016) - Reliability *(p.2440)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-252: Unchecked Return Value *(p.606)*
  - CWE-396: Declaration of Catch for Generic Exception *(p.959)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.961)*
  - CWE-456: Missing Initialization of a Variable *(p.1089)*
  - CWE-674: Uncontrolled Recursion *(p.1484)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-788: Access of Memory Location After End of Buffer *(p.1669)*
  - CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor *(p.1880)*
  - CWE-1047: Modules with Circular Dependencies *(p.1882)*
  - CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
  - CWE-1056: Invokable Control Element with Variadic Parameters *(p.1891)*
  - CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
  - CWE-1062: Parent Class with References to Child Class *(p.1900)*
  - CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers *(p.1903)*
  - CWE-1066: Missing Serialization Control Element *(p.1904)*
  - CWE-1069: Empty Exception Block *(p.1907)*
  - CWE-1070: Serializable Data Element Containing non-Serializable Item Elements *(p.1909)*
  - CWE-1077: Floating Point Comparison with Incorrect Operator *(p.1917)*
  - CWE-1079: Parent Class without Virtual Destructor Method *(p.1919)*
  - CWE-1082: Class Instance Self Destruction Control Element *(p.1921)*
  - CWE-1083: Data Access from Outside Expected Data Manager Component *(p.1922)*
  - CWE-1087: Class with Virtual Method without a Virtual Destructor *(p.1927)*
  - CWE-1088: Synchronous Access of Remote Resource without Timeout *(p.1928)*
  - CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element *(p.1937)*
  - CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*
  - CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element *(p.1938)*
- CWE-1130: CISQ Quality Measures (2016) - Maintainability *(p.2441)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-1041: Use of Redundant Code *(p.1875)*
  - CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range *(p.1879)*
  - CWE-1047: Modules with Circular Dependencies *(p.1882)*
  - CWE-1048: Invokable Control Element with Large Number of Outward Calls *(p.1883)*
  - CWE-1052: Excessive Use of Hard-Coded Literals in Initialization *(p.1887)*
  - CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer *(p.1889)*
  - CWE-1055: Multiple Inheritance from Concrete Classes *(p.1890)*
  - CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters *(p.1902)*
  - CWE-1074: Class with Excessively Deep Inheritance *(p.1914)*
  - CWE-1075: Unconditional Control Flow Transfer outside of Switch Block *(p.1915)*
  - CWE-1080: Source Code File with Excessive Number of Lines of Code *(p.1920)*
  - CWE-766: Critical Data Element Declared Public *(p.1607)*
  - CWE-1084: Invokable Control Element with Excessive File or Data Access Operations *(p.1924)*
  - CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code *(p.1925)*
  - CWE-1086: Class with Excessive Number of Child Classes *(p.1926)*
  - CWE-1090: Method Containing Access of a Member Element from Another Class *(p.1930)*
  - CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers *(p.1932)*

- CWE-1095: Loop Condition Value Update within the Loop *(p.1935)*
- CWE-1121: Excessive McCabe Cyclomatic Complexity *(p.1961)*

CWE-1131: CISQ Quality Measures (2016) - Security *(p.2442)*

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
- CWE-129: Improper Validation of Array Index *(p.341)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
- CWE-396: Declaration of Catch for Generic Exception *(p.959)*
- CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-456: Missing Initialization of a Variable *(p.1089)*
- CWE-606: Unchecked Input for Loop Condition *(p.1357)*
- CWE-667: Improper Locking *(p.1464)*
- CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*

CWE-1132: CISQ Quality Measures (2016) - Performance Efficiency *(p.2443)*

- CWE-1042: Static Member Data Element outside of a Singleton Class Element *(p.1876)*
- CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1877)*
- CWE-1046: Creation of Immutable Text Using String Concatenation *(p.1881)*
- CWE-1049: Excessive Data Query Operations in a Large Data Table *(p.1884)*
- CWE-1050: Excessive Platform Resource Consumption within a Loop *(p.1885)*
- CWE-1057: Data Access Operations Outside of Expected Data Manager Component *(p.1892)*
- CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses *(p.1897)*
- CWE-1063: Creation of Class Instance within a Static Code Block *(p.1901)*
- CWE-1067: Excessive Execution of Sequential Searches of Data Resource *(p.1905)*
- CWE-1072: Data Resource Access without Use of Connection Pooling *(p.1912)*
- CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses *(p.1913)*
- CWE-1089: Large Data Table with Excessive Number of Indices *(p.1929)*
- CWE-1091: Use of Object without Invoking Destructor Method *(p.1931)*
- CWE-1094: Excessive Index Range Scan for a Data Resource *(p.1934)*

Graph View: CWE-1133: Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java

- CWE-1134: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 00. Input Validation and Data Sanitization (IDS) *(p.2444)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.281)*
  - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.703)*
  - CWE-117: Improper Output Neutralization for Logs *(p.288)*
  - CWE-144: Improper Neutralization of Line Delimiters *(p.383)*
  - CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences *(p.394)*
  - CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.996)*
  - CWE-134: Use of Externally-Controlled Format String *(p.365)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-182: Collapse of Data into Unsafe Value *(p.455)*
- CWE-1135: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 01. Declarations and Initialization (DCL) *(p.2444)*
  - CWE-665: Improper Initialization *(p.1456)*
- CWE-1136: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 02. Expressions (EXP) *(p.2445)*
  - CWE-252: Unchecked Return Value *(p.606)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
  - CWE-595: Comparison of Object References Instead of Object Contents *(p.1334)*
- CWE-1137: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 03. Numeric Types and Operations (NUM) *(p.2445)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-191: Integer Underflow (Wrap or Wraparound) *(p.480)*
  - CWE-197: Numeric Truncation Error *(p.500)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-682: Incorrect Calculation *(p.1499)*
- CWE-1138: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 04. Characters and Strings (STR) *(p.2446)*
  - CWE-838: Inappropriate Encoding for Output Context *(p.1764)*
- CWE-1139: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 05. Object Orientation (OBJ) *(p.2446)*
  - CWE-374: Passing Mutable Objects to an Untrusted Method *(p.920)*
  - CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
  - CWE-486: Comparison of Classes by Name *(p.1164)*
  - CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1174)*
  - CWE-492: Use of Inner Class Containing Sensitive Data *(p.1175)*
  - CWE-498: Cloneable Class Containing Sensitive Information *(p.1196)*
  - CWE-500: Public Static Field Not Marked Final *(p.1200)*
  - CWE-766: Critical Data Element Declared Public *(p.1607)*
- CWE-1140: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 06. Methods (MET) *(p.2447)*
  - CWE-617: Reachable Assertion *(p.1378)*
  - CWE-589: Call to Non-ubiquitous API *(p.1325)*
  - CWE-697: Incorrect Comparison *(p.1530)*
  - CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*
  - CWE-573: Improper Following of Specification by Caller *(p.1298)*
  - CWE-586: Explicit Call to Finalize() *(p.1320)*
  - CWE-583: finalize() Method Declared Public *(p.1315)*
  - CWE-568: finalize() Method Without super.finalize() *(p.1290)*

- CWE-1141: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 07. Exceptional Behavior (ERR) *(p.2448)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
  - CWE-584: Return Inside Finally Block *(p.1317)*
  - CWE-459: Incomplete Cleanup *(p.1099)*
  - CWE-248: Uncaught Exception *(p.596)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1542)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
  - CWE-397: Declaration of Throws for Generic Exception *(p.961)*
  - CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
- CWE-1142: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 08. Visibility and Atomicity (VNA) *(p.2448)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-366: Race Condition within a Thread *(p.904)*
  - CWE-413: Improper Resource Locking *(p.1003)*
  - CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
  - CWE-662: Improper Synchronization *(p.1448)*
  - CWE-667: Improper Locking *(p.1464)*
- CWE-1143: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 09. Locking (LCK) *(p.2449)*
  - CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
  - CWE-609: Double-Checked Locking *(p.1362)*
  - CWE-667: Improper Locking *(p.1464)*
  - CWE-820: Missing Synchronization *(p.1720)*
- CWE-1144: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 10. Thread APIs (THI) *(p.2449)*
  - CWE-572: Call to Thread run() instead of start() *(p.1296)*
- CWE-1145: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 11. Thread Pools (TPS) *(p.2450)*
  - CWE-392: Missing Report of Error Condition *(p.951)*
  - CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
  - CWE-410: Insufficient Resource Pool *(p.998)*
- CWE-1146: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 12. Thread-Safety Miscellaneous (TSM) *(p.2450)*
- CWE-1147: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 13. Input Output (FIO) *(p.2450)*
  - CWE-67: Improper Handling of Windows Device Names *(p.126)*
  - CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
  - CWE-198: Use of Incorrect Byte Ordering *(p.503)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
  - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
  - CWE-377: Insecure Temporary File *(p.925)*
  - CWE-404: Improper Resource Shutdown or Release *(p.980)*
  - CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
  - CWE-459: Incomplete Cleanup *(p.1099)*
  - CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
  - CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1426)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1542)*
  - CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
  - CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-1148: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 14. Serialization (SER) *(p.2451)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
  - CWE-400: Uncontrolled Resource Consumption *(p.964)*

- V CWE-499: Serializable Class Containing Sensitive Data *(p.1198)*
- B CWE-502: Deserialization of Untrusted Data *(p.1204)*
- B CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*

C CWE-1149: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 15. Platform Security (SEC) *(p.2452)*
- B CWE-266: Incorrect Privilege Assignment *(p.638)*
- B CWE-272: Least Privilege Violation *(p.656)*
- C CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*

C CWE-1150: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 16. Runtime Environment (ENV) *(p.2452)*
- B CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- C CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*

C CWE-1151: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 17. Java Native Interface (JNI) *(p.2453)*
- V CWE-111: Direct Use of Unsafe JNI *(p.266)*

C CWE-1152: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 49. Miscellaneous (MSC) *(p.2453)*
- V CWE-259: Use of Hard-coded Password *(p.623)*
- C CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- C CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
- C CWE-330: Use of Insufficiently Random Values *(p.814)*
- V CWE-332: Insufficient Entropy in PRNG *(p.823)*
- V CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
- V CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
- C CWE-400: Uncontrolled Resource Consumption *(p.964)*
- V CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- B CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- B CWE-798: Use of Hard-coded Credentials *(p.1690)*

C CWE-1153: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 50. Android (DRD) *(p.2454)*

C CWE-1175: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 18. Concurrency (CON) *(p.2464)*

Graph View: CWE-1154: Weaknesses Addressed by the SEI CERT C Coding Standard

- CWE-1155: SEI CERT C Coding Standard - Guidelines 01. Preprocessor (PRE) *(p.2454)*
- CWE-1156: SEI CERT C Coding Standard - Guidelines 02. Declarations and Initialization (DCL) *(p.2455)*
  - CWE-562: Return of Stack Variable Address *(p.1278)*
- CWE-1157: SEI CERT C Coding Standard - Guidelines 03. Expressions (EXP) *(p.2455)*
  - CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
  - CWE-908: Use of Uninitialized Resource *(p.1792)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1514)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
  - CWE-685: Function Call With Incorrect Number of Arguments *(p.1507)*
  - CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
  - CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') *(p.1776)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-125: Out-of-bounds Read *(p.330)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
  - CWE-481: Assigning instead of Comparing *(p.1154)*
- CWE-1158: SEI CERT C Coding Standard - Guidelines 04. Integers (INT) *(p.2456)*
  - CWE-190: Integer Overflow or Wraparound *(p.472)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-191: Integer Underflow (Wrap or Wraparound) *(p.480)*
  - CWE-680: Integer Overflow to Buffer Overflow *(p.1493)*
  - CWE-192: Integer Coercion Error *(p.482)*
  - CWE-197: Numeric Truncation Error *(p.500)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
  - CWE-194: Unexpected Sign Extension *(p.491)*
  - CWE-195: Signed to Unsigned Conversion Error *(p.494)*
  - CWE-369: Divide By Zero *(p.913)*
  - CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
  - CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*
- CWE-1159: SEI CERT C Coding Standard - Guidelines 05. Floating Point (FLP) *(p.2457)*
  - CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-197: Numeric Truncation Error *(p.500)*
- CWE-1160: SEI CERT C Coding Standard - Guidelines 06. Arrays (ARR) *(p.2457)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-786: Access of Memory Location Before Start of Buffer *(p.1658)*
  - CWE-123: Write-what-where Condition *(p.323)*
  - CWE-125: Out-of-bounds Read *(p.330)*
  - CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
  - CWE-469: Use of Pointer Subtraction to Determine Size *(p.1115)*
  - CWE-121: Stack-based Buffer Overflow *(p.314)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
  - CWE-468: Incorrect Pointer Scaling *(p.1114)*
- CWE-1161: SEI CERT C Coding Standard - Guidelines 07. Characters and Strings (STR) *(p.2458)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*

- CWE-121: Stack-based Buffer Overflow *(p.314)*
- CWE-122: Heap-based Buffer Overflow *(p.318)*
- CWE-123: Write-what-where Condition *(p.323)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-170: Improper Null Termination *(p.428)*
- CWE-704: Incorrect Type Conversion or Cast *(p.1538)*

CWE-1162: SEI CERT C Coding Standard - Guidelines 08. Memory Management (MEM) *(p.2458)*
- CWE-416: Use After Free *(p.1012)*
- CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
- CWE-666: Operation on Resource in Wrong Phase of Lifetime *(p.1462)*
- CWE-415: Double Free *(p.1008)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-459: Incomplete Cleanup *(p.1099)*
- CWE-771: Missing Reference to Active Allocated Resource *(p.1622)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-590: Free of Memory not on the Heap *(p.1326)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
- CWE-680: Integer Overflow to Buffer Overflow *(p.1493)*
- CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
- CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*

CWE-1163: SEI CERT C Coding Standard - Guidelines 09. Input Output (FIO) *(p.2459)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-67: Improper Handling of Windows Device Names *(p.126)*
- CWE-197: Numeric Truncation Error *(p.500)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-664: Improper Control of a Resource Through its Lifetime *(p.1454)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-459: Incomplete Cleanup *(p.1099)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-773: Missing Reference to Active File Descriptor or Handle *(p.1629)*
- CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
- CWE-771: Missing Reference to Active Allocated Resource *(p.1622)*
- CWE-910: Use of Expired File Descriptor *(p.1800)*
- CWE-666: Operation on Resource in Wrong Phase of Lifetime *(p.1462)*
- CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
- CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
- CWE-685: Function Call With Incorrect Number of Arguments *(p.1507)*

CWE-1165: SEI CERT C Coding Standard - Guidelines 10. Environment (ENV) *(p.2460)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*

CWE-1166: SEI CERT C Coding Standard - Guidelines 11. Signals (SIG) *(p.2460)*
- CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
- CWE-662: Improper Synchronization *(p.1448)*

CWE-1167: SEI CERT C Coding Standard - Guidelines 12. Error Handling (ERR) *(p.2461)*
- CWE-456: Missing Initialization of a Variable *(p.1089)*

- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-253: Incorrect Check of Function Return Value *(p.613)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*

CWE-1168: SEI CERT C Coding Standard - Guidelines 13. Application Programming Interfaces (API) *(p.2462)*

CWE-1169: SEI CERT C Coding Standard - Guidelines 14. Concurrency (CON) *(p.2462)*

- CWE-667: Improper Locking *(p.1464)*
- CWE-366: Race Condition within a Thread *(p.904)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
- CWE-377: Insecure Temporary File *(p.925)*

CWE-1170: SEI CERT C Coding Standard - Guidelines 48. Miscellaneous (MSC) *(p.2463)*

- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-331: Insufficient Entropy *(p.821)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*

CWE-1171: SEI CERT C Coding Standard - Guidelines 50. POSIX (POS) *(p.2463)*

- CWE-170: Improper Null Termination *(p.428)*
- CWE-242: Use of Inherently Dangerous Function *(p.586)*
- CWE-363: Race Condition Enabling Link Following *(p.897)*
- CWE-696: Incorrect Behavior Order *(p.1527)*
- CWE-273: Improper Check for Dropped Privileges *(p.660)*
- CWE-667: Improper Locking *(p.1464)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-253: Incorrect Check of Function Return Value *(p.613)*

CWE-1172: SEI CERT C Coding Standard - Guidelines 51. Microsoft Windows (WIN) *(p.2464)*

- CWE-762: Mismatched Memory Management Routines *(p.1596)*
- CWE-590: Free of Memory not on the Heap *(p.1326)*

Graph View: CWE-1178: Weaknesses Addressed by the SEI CERT Perl Coding Standard

- CWE-1179: SEI CERT Perl Coding Standard - Guidelines 01. Input Validation and Data Sanitization (IDS) *(p.2465)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-134: Use of Externally-Controlled Format String *(p.365)*
  - CWE-129: Improper Validation of Array Index *(p.341)*
  - CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
  - CWE-116: Improper Encoding or Escaping of Output *(p.281)*
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
- CWE-1180: SEI CERT Perl Coding Standard - Guidelines 02. Declarations and Initialization (DCL) *(p.2465)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
  - CWE-456: Missing Initialization of a Variable *(p.1089)*
  - CWE-457: Use of Uninitialized Variable *(p.1094)*
  - CWE-477: Use of Obsolete Function *(p.1138)*
- CWE-1181: SEI CERT Perl Coding Standard - Guidelines 03. Expressions (EXP) *(p.2466)*
  - CWE-394: Unexpected Status Code or Return Value *(p.955)*
  - CWE-783: Operator Precedence Logic Error *(p.1650)*
  - CWE-477: Use of Obsolete Function *(p.1138)*
  - CWE-248: Uncaught Exception *(p.596)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
  - CWE-705: Incorrect Control Flow Scoping *(p.1542)*
  - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
  - CWE-252: Unchecked Return Value *(p.606)*
  - CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1514)*
  - CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
  - CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
  - CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
- CWE-1182: SEI CERT Perl Coding Standard - Guidelines 04. Integers (INT) *(p.2466)*
  - CWE-189: Numeric Errors *(p.2312)*
- CWE-1183: SEI CERT Perl Coding Standard - Guidelines 05. Strings (STR) *(p.2467)*
- CWE-1184: SEI CERT Perl Coding Standard - Guidelines 06. Object-Oriented Programming (OOP) *(p.2467)*
  - CWE-767: Access to Critical Private Variable via Public Method *(p.1610)*
- CWE-1185: SEI CERT Perl Coding Standard - Guidelines 07. File Input and Output (FIO) *(p.2468)*
  - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
- CWE-1186: SEI CERT Perl Coding Standard - Guidelines 50. Miscellaneous (MSC) *(p.2468)*
  - CWE-561: Dead Code *(p.1275)*
  - CWE-563: Assignment to Variable without Use *(p.1280)*

Graph View: CWE-1194: Hardware Design

- CWE-1195: Manufacturing and Life Cycle Management Concerns *(p.2469)*
  - CWE-1059: Insufficient Technical Documentation *(p.1894)*
  - CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications *(p.2049)*
  - CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device *(p.2091)*
  - CWE-1269: Product Released in Non-Release Configuration *(p.2098)*
  - CWE-1273: Device Unlock Credential Sharing *(p.2106)*
  - CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT Vendors *(p.2156)*
- CWE-1196: Security Flow Issues *(p.2469)*
  - CWE-1190: DMA Device Enabled Too Early in Boot Phase *(p.1978)*
  - CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control *(p.1986)*
  - CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels *(p.2086)*
  - CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code *(p.2108)*
  - CWE-1283: Mutable Attestation or Measurement Reporting Data *(p.2128)*
  - CWE-1310: Missing Ability to Patch ROM Code *(p.2179)*
  - CWE-1326: Missing Immutable Root of Trust in Hardware *(p.2212)*
  - CWE-1328: Security Version Number Mutable to Older Versions *(p.2217)*
- CWE-1197: Integration Issues *(p.2470)*
  - CWE-1276: Hardware Child Block Incorrectly Connected to Parent System *(p.2113)*
- CWE-1198: Privilege Separation and Access Control Issues *(p.2470)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1064)*
  - CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
  - CWE-1192: Improper Identifier for IP Block used in System-On-Chip (SOC) *(p.1985)*
  - CWE-1220: Insufficient Granularity of Access Control *(p.1992)*
  - CWE-1222: Insufficient Granularity of Address Regions Protected by Register Locks *(p.1999)*
  - CWE-1242: Inclusion of Undocumented Features or Chicken Bits *(p.2033)*
  - CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges *(p.2075)*
  - CWE-1262: Improper Access Control for Register Interface *(p.2081)*
  - CWE-1267: Policy Uses Obsolete Encoding *(p.2093)*
  - CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents *(p.2095)*
  - CWE-1280: Access Control Check Implemented After Asset is Accessed *(p.2122)*
  - CWE-1294: Insecure Security Identifier Mechanism *(p.2150)*
    - CWE-1259: Improper Restriction of Security Token Assignment *(p.2073)*
    - CWE-1270: Generation of Incorrect Security Tokens *(p.2100)*
    - CWE-1290: Incorrect Decoding of Security Identifiers *(p.2142)*
    - CWE-1292: Incorrect Conversion of Security Identifiers *(p.2147)*
  - CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface *(p.2162)*
  - CWE-1302: Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC) *(p.2172)*
  - CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
  - CWE-1314: Missing Write Protection for Parametric Data Values *(p.2187)*
  - CWE-1318: Missing Support for Security Features in On-chip Fabrics or Buses *(p.2197)*
  - CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy *(p.2234)*
  - CWE-1420: Exposure of Sensitive Information during Transient Execution *(p.2284)*
    - CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution *(p.2290)*
    - CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution *(p.2297)*
    - CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution *(p.2302)*
- CWE-1199: General Circuit and Logic Design Concerns *(p.2471)*
  - CWE-1209: Failure to Disable Reserved Bits *(p.1991)*
  - CWE-1221: Incorrect Register Defaults or Module Parameters *(p.1996)*

- CWE-1223: Race Condition for Write-Once Attributes *(p.2001)*
- CWE-1224: Improper Restriction of Write-Once Bit Fields *(p.2003)*
- CWE-1231: Improper Prevention of Lock Bit Modification *(p.2007)*
- CWE-1232: Improper Lock Behavior After Power State Transition *(p.2010)*
- CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2012)*
- CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks *(p.2014)*
- CWE-1245: Improper Finite State Machines (FSMs) in Hardware Logic *(p.2041)*
- CWE-1250: Improper Preservation of Consistency Between Independent Representations of Shared State *(p.2052)*
- CWE-1253: Incorrect Selection of Fuse Values *(p.2058)*
- CWE-1254: Incorrect Comparison Logic Granularity *(p.2060)*
- CWE-1261: Improper Handling of Single Event Upsets *(p.2079)*
- CWE-1298: Hardware Logic Contains Race Conditions *(p.2158)*

CWE-1201: Core and Compute Issues *(p.2471)*
- CWE-1252: CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations *(p.2056)*
- CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior *(p.2124)*
- CWE-1342: Information Exposure through Microarchitectural State after Transient Execution *(p.2250)*
- CWE-1420: Exposure of Sensitive Information during Transient Execution *(p.2284)*
  - CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution *(p.2290)*
  - CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution *(p.2297)*
  - CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution *(p.2302)*

CWE-1202: Memory and Storage Issues *(p.2472)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
  - CWE-1239: Improper Zeroization of Hardware Register *(p.2022)*
  - CWE-1342: Information Exposure through Microarchitectural State after Transient Execution *(p.2250)*
- CWE-1246: Improper Write Handling in Limited-write Non-Volatile Memories *(p.2043)*
- CWE-1251: Mirrored Regions with Different Values *(p.2054)*
- CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions *(p.2068)*
- CWE-1282: Assumed-Immutable Data is Stored in Writable Memory *(p.2127)*
- CWE-1420: Exposure of Sensitive Information during Transient Execution *(p.2284)*
  - CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution *(p.2290)*
  - CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution *(p.2297)*
  - CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution *(p.2302)*

CWE-1203: Peripherals, On-chip Fabric, and Interface/IO Problems *(p.2472)*
- CWE-1311: Improper Translation of Security Attributes by Fabric Bridge *(p.2182)*
- CWE-1312: Missing Protection for Mirrored Regions in On-Chip Fabric Firewall *(p.2184)*
- CWE-1315: Improper Setting of Bus Controlling Capability in Fabric End-point *(p.2190)*
- CWE-1316: Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges *(p.2192)*
- CWE-1317: Improper Access Control in Fabric Bridge *(p.2194)*
- CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) *(p.2225)*

CWE-1205: Security Primitives and Cryptography Issues *(p.2473)*
- CWE-203: Observable Discrepancy *(p.518)*
  - CWE-1300: Improper Protection of Physical Side Channels *(p.2165)*
- CWE-325: Missing Cryptographic Step *(p.794)*
- CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation *(p.2025)*
- CWE-1241: Use of Predictable Algorithm in Random Number Generator *(p.2030)*
- CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready *(p.2120)*
- CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments *(p.2252)*

- CWE-1206: Power, Clock, Thermal, and Reset Concerns *(p.2473)*
  - CWE-1232: Improper Lock Behavior After Power State Transition *(p.2010)*
  - CWE-1247: Improper Protection Against Voltage and Clock Glitches *(p.2044)*
  - CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications *(p.2049)*
  - CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks *(p.2062)*
  - CWE-1256: Improper Restriction of Software Interfaces to Hardware Features *(p.2065)*
  - CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings *(p.2102)*
  - CWE-1304: Improperly Preserved Integrity of Hardware Configuration State During a Power Save/ Restore Operation *(p.2176)*
  - CWE-1314: Missing Write Protection for Parametric Data Values *(p.2187)*
  - CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals *(p.2202)*
  - CWE-1332: Improper Handling of Faults that Lead to Instruction Skips *(p.2227)*
  - CWE-1338: Improper Protections Against Hardware Overheating *(p.2240)*
- CWE-1207: Debug and Test Problems *(p.2474)*
  - CWE-1191: On-Chip Debug and Test Interface With Improper Access Control *(p.1980)*
  - CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks *(p.2014)*
  - CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug *(p.2035)*
  - CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State *(p.2037)*
  - CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information *(p.2071)*
  - CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition *(p.2104)*
  - CWE-1291: Public Key Re-Use for Signing both Debug and Production Code *(p.2145)*
  - CWE-1295: Debug Messages Revealing Unnecessary Information *(p.2152)*
  - CWE-1296: Incorrect Chaining or Granularity of Debug Components *(p.2153)*
  - CWE-1313: Hardware Allows Activation of Test or Debug Logic at Runtime *(p.2185)*
  - CWE-1323: Improper Management of Sensitive Trace Data *(p.2208)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-1208: Cross-Cutting Problems *(p.2474)*
  - CWE-440: Expected Behavior Violation *(p.1062)*
  - CWE-1053: Missing Documentation for Design *(p.1888)*
  - CWE-1059: Insufficient Technical Documentation *(p.1894)*
  - CWE-1263: Improper Physical Access Control *(p.2085)*
  - CWE-1277: Firmware Not Updateable *(p.2116)*
  - CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component *(p.2170)*
    - CWE-1330: Remanent Data Readable after Memory Erase *(p.2222)*
  - CWE-1329: Reliance on Component That is Not Updateable *(p.2219)*
  - CWE-1357: Reliance on Insufficiently Trustworthy Component *(p.2254)*
- CWE-1388: Physical Access Issues and Concerns *(p.2518)*
  - CWE-1384: Improper Handling of Physical or Environmental Conditions *(p.2257)*
  - CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) *(p.2199)*
  - CWE-1247: Improper Protection Against Voltage and Clock Glitches *(p.2044)*
  - CWE-1261: Improper Handling of Single Event Upsets *(p.2079)*
  - CWE-1332: Improper Handling of Faults that Lead to Instruction Skips *(p.2227)*
  - CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments *(p.2252)*
  - CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques *(p.2118)*
  - CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks *(p.2062)*
  - CWE-1300: Improper Protection of Physical Side Channels *(p.2165)*
  - CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications *(p.2049)*

Graph View: CWE-1200: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-416: Use After Free *(p.1012)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-269: Improper Privilege Management *(p.646)*
- CWE-295: Improper Certificate Validation *(p.714)*

Graph View: CWE-1305: CISQ Quality Measures (2020)

- CWE-1306: CISQ Quality Measures - Reliability *(p.2483)*
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
    - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
    - CWE-123: Write-what-where Condition *(p.323)*
    - CWE-125: Out-of-bounds Read *(p.330)*
    - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
    - CWE-786: Access of Memory Location Before Start of Buffer *(p.1658)*
    - CWE-787: Out-of-bounds Write *(p.1661)*
    - CWE-788: Access of Memory Location After End of Buffer *(p.1669)*
    - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
    - CWE-822: Untrusted Pointer Dereference *(p.1723)*
    - CWE-823: Use of Out-of-range Pointer Offset *(p.1726)*
    - CWE-824: Access of Uninitialized Pointer *(p.1729)*
    - CWE-825: Expired Pointer Dereference *(p.1732)*
  - CWE-170: Improper Null Termination *(p.428)*
  - CWE-252: Unchecked Return Value *(p.606)*
  - CWE-390: Detection of Error Condition Without Action *(p.943)*
  - CWE-394: Unexpected Status Code or Return Value *(p.955)*
  - CWE-404: Improper Resource Shutdown or Release *(p.980)*
    - CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
    - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
    - CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
  - CWE-424: Improper Protection of Alternate Path *(p.1023)*
  - CWE-459: Incomplete Cleanup *(p.1099)*
  - CWE-476: NULL Pointer Dereference *(p.1132)*
  - CWE-480: Use of Incorrect Operator *(p.1150)*
  - CWE-484: Omitted Break Statement in Switch *(p.1162)*
  - CWE-562: Return of Stack Variable Address *(p.1278)*
  - CWE-595: Comparison of Object References Instead of Object Contents *(p.1334)*
    - CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element *(p.1937)*
    - CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
  - CWE-662: Improper Synchronization *(p.1448)*
    - CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
    - CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*
    - CWE-366: Race Condition within a Thread *(p.904)*
    - CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
    - CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
    - CWE-667: Improper Locking *(p.1464)*
    - CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
    - CWE-820: Missing Synchronization *(p.1720)*
    - CWE-821: Incorrect Synchronization *(p.1722)*
    - CWE-833: Deadlock *(p.1753)*
  - CWE-665: Improper Initialization *(p.1456)*
    - CWE-456: Missing Initialization of a Variable *(p.1089)*
    - CWE-457: Use of Uninitialized Variable *(p.1094)*
  - CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
    - CWE-415: Double Free *(p.1008)*
    - CWE-416: Use After Free *(p.1012)*
  - CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
    - CWE-194: Unexpected Sign Extension *(p.491)*
    - CWE-195: Signed to Unsigned Conversion Error *(p.494)*

- CWE-196: Unsigned to Signed Conversion Error *(p.498)*
- CWE-197: Numeric Truncation Error *(p.500)*
- CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-369: Divide By Zero *(p.913)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
  - CWE-248: Uncaught Exception *(p.596)*
  - CWE-391: Unchecked Error Condition *(p.948)*
  - CWE-392: Missing Report of Error Condition *(p.951)*
- CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
- CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*
- CWE-908: Use of Uninitialized Resource *(p.1792)*
- CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor *(p.1880)*
- CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
- CWE-1066: Missing Serialization Control Element *(p.1904)*
- CWE-1070: Serializable Data Element Containing non-Serializable Item Elements *(p.1909)*
- CWE-1077: Floating Point Comparison with Incorrect Operator *(p.1917)*
- CWE-1079: Parent Class without Virtual Destructor Method *(p.1919)*
- CWE-1082: Class Instance Self Destruction Control Element *(p.1921)*
- CWE-1083: Data Access from Outside Expected Data Manager Component *(p.1922)*
- CWE-1087: Class with Virtual Method without a Virtual Destructor *(p.1927)*
- CWE-1088: Synchronous Access of Remote Resource without Timeout *(p.1928)*
- CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element *(p.1938)*

CWE-1307: CISQ Quality Measures - Maintainability *(p.2484)*

- CWE-407: Inefficient Algorithmic Complexity *(p.992)*
- CWE-478: Missing Default Case in Multiple Condition Expression *(p.1142)*
- CWE-480: Use of Incorrect Operator *(p.1150)*
- CWE-484: Omitted Break Statement in Switch *(p.1162)*
- CWE-561: Dead Code *(p.1275)*
- CWE-570: Expression is Always False *(p.1292)*
- CWE-571: Expression is Always True *(p.1295)*
- CWE-783: Operator Precedence Logic Error *(p.1650)*
- CWE-1041: Use of Redundant Code *(p.1875)*
- CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor *(p.1880)*
- CWE-1047: Modules with Circular Dependencies *(p.1882)*
- CWE-1048: Invokable Control Element with Large Number of Outward Calls *(p.1883)*
- CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
- CWE-1052: Excessive Use of Hard-Coded Literals in Initialization *(p.1887)*
- CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer *(p.1889)*
- CWE-1055: Multiple Inheritance from Concrete Classes *(p.1890)*
- CWE-1062: Parent Class with References to Child Class *(p.1900)*
- CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters *(p.1902)*
- CWE-1074: Class with Excessively Deep Inheritance *(p.1914)*
- CWE-1075: Unconditional Control Flow Transfer outside of Switch Block *(p.1915)*
- CWE-1079: Parent Class without Virtual Destructor Method *(p.1919)*
- CWE-1080: Source Code File with Excessive Number of Lines of Code *(p.1920)*
- CWE-1084: Invokable Control Element with Excessive File or Data Access Operations *(p.1924)*
- CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code *(p.1925)*
- CWE-1086: Class with Excessive Number of Child Classes *(p.1926)*
- CWE-1087: Class with Virtual Method without a Virtual Destructor *(p.1927)*
- CWE-1090: Method Containing Access of a Member Element from Another Class *(p.1930)*

- CWE-1095: Loop Condition Value Update within the Loop *(p.1935)*

CWE-1308: CISQ Quality Measures - Security *(p.2485)*

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-23: Relative Path Traversal *(p.46)*
  - CWE-36: Absolute Path Traversal *(p.75)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-624: Executable Regular Expression Error *(p.1390)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
  - CWE-564: SQL Injection: Hibernate *(p.1282)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-123: Write-what-where Condition *(p.323)*
  - CWE-125: Out-of-bounds Read *(p.330)*
  - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
  - CWE-786: Access of Memory Location Before Start of Buffer *(p.1658)*
  - CWE-787: Out-of-bounds Write *(p.1661)*
  - CWE-788: Access of Memory Location After End of Buffer *(p.1669)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
  - CWE-822: Untrusted Pointer Dereference *(p.1723)*
  - CWE-823: Use of Out-of-range Pointer Offset *(p.1726)*
  - CWE-824: Access of Uninitialized Pointer *(p.1729)*
  - CWE-825: Expired Pointer Dereference *(p.1732)*
- CWE-129: Improper Validation of Array Index *(p.341)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
  - CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
- CWE-424: Improper Protection of Alternate Path *(p.1023)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-477: Use of Obsolete Function *(p.1138)*
- CWE-480: Use of Incorrect Operator *(p.1150)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-570: Expression is Always False *(p.1292)*
- CWE-571: Expression is Always True *(p.1295)*
- CWE-606: Unchecked Input for Loop Condition *(p.1357)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
- CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
- CWE-662: Improper Synchronization *(p.1448)*
  - CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*

- CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*
- CWE-366: Race Condition within a Thread *(p.904)*
- CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
- CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
- CWE-667: Improper Locking *(p.1464)*
- CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
- CWE-820: Missing Synchronization *(p.1720)*
- CWE-821: Incorrect Synchronization *(p.1722)*
- CWE-833: Deadlock *(p.1753)*
- CWE-665: Improper Initialization *(p.1456)*
  - CWE-456: Missing Initialization of a Variable *(p.1089)*
  - CWE-457: Use of Uninitialized Variable *(p.1094)*
- CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
  - CWE-415: Double Free *(p.1008)*
  - CWE-416: Use After Free *(p.1012)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-194: Unexpected Sign Extension *(p.491)*
  - CWE-195: Signed to Unsigned Conversion Error *(p.494)*
  - CWE-196: Unsigned to Signed Conversion Error *(p.498)*
  - CWE-197: Numeric Truncation Error *(p.500)*
- CWE-682: Incorrect Calculation *(p.1499)*
  - CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
  - CWE-369: Divide By Zero *(p.913)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-778: Insufficient Logging *(p.1638)*
- CWE-783: Operator Precedence Logic Error *(p.1650)*
- CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*

CWE-1309: CISQ Quality Measures - Efficiency *(p.2486)*

- CWE-404: Improper Resource Shutdown or Release *(p.980)*
  - CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
- CWE-424: Improper Protection of Alternate Path *(p.1023)*
- CWE-1042: Static Member Data Element outside of a Singleton Class Element *(p.1876)*
- CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1877)*
- CWE-1046: Creation of Immutable Text Using String Concatenation *(p.1881)*
- CWE-1049: Excessive Data Query Operations in a Large Data Table *(p.1884)*
- CWE-1050: Excessive Platform Resource Consumption within a Loop *(p.1885)*
- CWE-1057: Data Access Operations Outside of Expected Data Manager Component *(p.1892)*
- CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses *(p.1897)*
- CWE-1067: Excessive Execution of Sequential Searches of Data Resource *(p.1905)*
- CWE-1072: Data Resource Access without Use of Connection Pooling *(p.1912)*
- CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses *(p.1913)*
- CWE-1089: Large Data Table with Excessive Number of Indices *(p.1929)*
- CWE-1091: Use of Object without Invoking Destructor Method *(p.1931)*
- CWE-1094: Excessive Index Range Scan for a Data Resource *(p.1934)*

Graph View: CWE-1337: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses

- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-416: Use After Free *(p.1012)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-306: Missing Authentication for Critical Function *(p.741)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-862: Missing Authorization *(p.1780)*
- CWE-276: Incorrect Default Permissions *(p.665)*
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*

Graph View: CWE-1340: CISQ Data Protection Measures

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
  - CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
  - CWE-123: Write-what-where Condition *(p.323)*
  - CWE-125: Out-of-bounds Read *(p.330)*
  - CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
  - CWE-786: Access of Memory Location Before Start of Buffer *(p.1658)*
  - CWE-787: Out-of-bounds Write *(p.1661)*
  - CWE-788: Access of Memory Location After End of Buffer *(p.1669)*
  - CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
  - CWE-822: Untrusted Pointer Dereference *(p.1723)*
  - CWE-823: Use of Out-of-range Pointer Offset *(p.1726)*
  - CWE-824: Access of Uninitialized Pointer *(p.1729)*
  - CWE-825: Expired Pointer Dereference *(p.1732)*
- CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
  - CWE-415: Double Free *(p.1008)*
  - CWE-416: Use After Free *(p.1012)*
- CWE-665: Improper Initialization *(p.1456)*
  - CWE-456: Missing Initialization of a Variable *(p.1089)*
  - CWE-457: Use of Uninitialized Variable *(p.1094)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
  - CWE-761: Free of Pointer not at Start of Buffer *(p.1592)*
  - CWE-762: Mismatched Memory Management Routines *(p.1596)*
  - CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
  - CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
  - CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
- CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
  - CWE-624: Executable Regular Expression Error *(p.1390)*
  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
  - CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
  - CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
- CWE-424: Improper Protection of Alternate Path *(p.1023)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
  - CWE-194: Unexpected Sign Extension *(p.491)*
  - CWE-195: Signed to Unsigned Conversion Error *(p.494)*
  - CWE-196: Unsigned to Signed Conversion Error *(p.498)*
  - CWE-197: Numeric Truncation Error *(p.500)*
- CWE-662: Improper Synchronization *(p.1448)*
  - CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
  - CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*

- CWE-366: Race Condition within a Thread *(p.904)*
- CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
- CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
- CWE-667: Improper Locking *(p.1464)*
- CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
- CWE-820: Missing Synchronization *(p.1720)*
- CWE-821: Incorrect Synchronization *(p.1722)*

CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
CWE-562: Return of Stack Variable Address *(p.1278)*
CWE-170: Improper Null Termination *(p.428)*
CWE-129: Improper Validation of Array Index *(p.341)*
CWE-134: Use of Externally-Controlled Format String *(p.365)*
CWE-606: Unchecked Input for Loop Condition *(p.1357)*
CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*

- CWE-23: Relative Path Traversal *(p.46)*
- CWE-36: Absolute Path Traversal *(p.75)*

CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*

- CWE-248: Uncaught Exception *(p.596)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-392: Missing Report of Error Condition *(p.951)*

CWE-908: Use of Uninitialized Resource *(p.1792)*
CWE-682: Incorrect Calculation *(p.1499)*

- CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
- CWE-369: Divide By Zero *(p.913)*

CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
CWE-502: Deserialization of Untrusted Data *(p.1204)*
CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.547)*
CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes *(p.1809)*
CWE-311: Missing Encryption of Sensitive Data *(p.757)*
CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
CWE-284: Improper Access Control *(p.680)*

- CWE-285: Improper Authorization *(p.684)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
- CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
- CWE-862: Missing Authorization *(p.1780)*
- CWE-863: Incorrect Authorization *(p.1787)*

Graph View: CWE-1344: Weaknesses in OWASP Top Ten (2021)

- CWE-1345: OWASP Top Ten 2021 Category A01:2021 - Broken Access Control *(p.2487)*
  - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
  - CWE-23: Relative Path Traversal *(p.46)*
  - CWE-35: Path Traversal: '.../.../..//' *(p.73)*
  - CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
  - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
  - CWE-201: Insertion of Sensitive Information Into Sent Data *(p.514)*
  - CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
  - CWE-264: Permissions, Privileges, and Access Controls *(p.2316)*
  - CWE-275: Permission Issues *(p.2317)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-284: Improper Access Control *(p.680)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
  - CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
  - CWE-377: Insecure Temporary File *(p.925)*
  - CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') *(p.976)*
  - CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
  - CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1064)*
  - CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
  - CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
  - CWE-540: Inclusion of Sensitive Information in Source Code *(p.1251)*
  - CWE-548: Exposure of Information Through Directory Listing *(p.1261)*
  - CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
  - CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1286)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
  - CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
  - CWE-651: Exposure of WSDL File Containing Sensitive Information *(p.1433)*
  - CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
  - CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1544)*
  - CWE-862: Missing Authorization *(p.1780)*
  - CWE-863: Incorrect Authorization *(p.1787)*
  - CWE-913: Improper Control of Dynamically-Managed Code Resources *(p.1805)*
  - CWE-922: Insecure Storage of Sensitive Information *(p.1825)*
  - CWE-1275: Sensitive Cookie with Improper SameSite Attribute *(p.2110)*
- CWE-1346: OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures *(p.2488)*
  - CWE-261: Weak Encoding for Password *(p.631)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
  - CWE-310: Cryptographic Issues *(p.2318)*
  - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
  - CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
  - CWE-322: Key Exchange without Entity Authentication *(p.788)*
  - CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.790)*
  - CWE-324: Use of a Key Past its Expiration Date *(p.792)*
  - CWE-325: Missing Cryptographic Step *(p.794)*
  - CWE-326: Inadequate Encryption Strength *(p.796)*
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
  - CWE-328: Use of Weak Hash *(p.806)*
  - CWE-329: Generation of Predictable IV with CBC Mode *(p.811)*
  - CWE-330: Use of Insufficiently Random Values *(p.814)*
  - CWE-331: Insufficient Entropy *(p.821)*

- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-340: Generation of Predictable Numbers or Identifiers *(p.842)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- CWE-523: Unprotected Transport of Credentials *(p.1230)*
- CWE-720: OWASP Top Ten 2007 Category A9 - Insecure Communications *(p.2333)*
- CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') *(p.1581)*
- CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
- CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1589)*
- CWE-780: Use of RSA Algorithm without OAEP *(p.1644)*
- CWE-818: OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection *(p.2359)*
- CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*

CWE-1347: OWASP Top Ten 2021 Category A03:2021 - Injection *(p.2490)*

- CWE-20: Improper Input Validation *(p.20)*
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
- CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) *(p.142)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) *(p.177)*
- CWE-83: Improper Neutralization of Script in Attributes in a Web Page *(p.183)*
- CWE-87: Improper Neutralization of Alternate XSS Syntax *(p.192)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
- CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.232)*
- CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.235)*
- CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.271)*
- CWE-116: Improper Encoding or Escaping of Output *(p.281)*
- CWE-138: Improper Neutralization of Special Elements *(p.373)*
- CWE-184: Incomplete List of Disallowed Inputs *(p.459)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-471: Modification of Assumed-Immutable Data (MAID) *(p.1121)*
- CWE-564: SQL Injection: Hibernate *(p.1282)*
- CWE-610: Externally Controlled Reference to a Resource in Another Sphere *(p.1364)*
- CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
- CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(p.1422)*
- CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*

- B CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*

C CWE-1348: OWASP Top Ten 2021 Category A04:2021 - Insecure Design *(p.2491)*
- B CWE-73: External Control of File Name or Path *(p.132)*
- B CWE-183: Permissive List of Allowed Inputs *(p.458)*
- B CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- B CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.547)*
- V CWE-235: Improper Handling of Extra Parameters *(p.578)*
- B CWE-256: Plaintext Storage of a Password *(p.615)*
- B CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
- B CWE-266: Incorrect Privilege Assignment *(p.638)*
- C CWE-269: Improper Privilege Management *(p.646)*
- B CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.672)*
- C CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- B CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
- V CWE-313: Cleartext Storage in a File or on Disk *(p.770)*
- V CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.775)*
- B CWE-419: Unprotected Primary Channel *(p.1017)*
- B CWE-430: Deployment of Wrong Handler *(p.1042)*
- B CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- B CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1068)*
- C CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1079)*
- B CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
- B CWE-501: Trust Boundary Violation *(p.1203)*
- C CWE-522: Insufficiently Protected Credentials *(p.1225)*
- V CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1233)*
- V CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1250)*
- V CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session *(p.1309)*
- V CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1340)*
- C CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
- C CWE-642: External Control of Critical State Data *(p.1414)*
- V CWE-646: Reliance on File Name or Extension of Externally-Supplied File *(p.1425)*
- V CWE-650: Trusting HTTP Permission Methods on the Server Side *(p.1432)*
- C CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
- C CWE-656: Reliance on Security Through Obscurity *(p.1444)*
- C CWE-657: Violation of Secure Design Principles *(p.1446)*
- C CWE-799: Improper Control of Interaction Frequency *(p.1699)*
- B CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
- C CWE-840: Business Logic Errors *(p.2360)*
- B CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*
- V CWE-927: Use of Implicit Intent for Sensitive Communication *(p.1836)*
- B CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
- B CWE-1173: Improper Use of Validation Framework *(p.1969)*

C CWE-1349: OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration *(p.2493)*
- C CWE-2: 7PK - Environment *(p.2308)*
- V CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
- V CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
- B CWE-15: External Control of System or Configuration Setting *(p.17)*
- C CWE-16: Configuration *(p.2309)*
- B CWE-260: Password in Configuration File *(p.629)*
- V CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.774)*
- V CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1222)*
- V CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1234)*

- CWE-537: Java Runtime Error Message Containing Sensitive Information *(p.1246)*
- CWE-541: Inclusion of Sensitive Information in an Include File *(p.1253)*
- CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1259)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute *(p.1373)*
- CWE-756: Missing Custom Error Page *(p.1579)*
- CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*
- CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1847)*
- CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag *(p.1854)*
- CWE-1032: OWASP Top Ten 2017 Category A6 - Security Misconfiguration *(p.2438)*
- CWE-1174: ASP.NET Misconfiguration: Improper Model Validation *(p.1970)*

CWE-1352: OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components *(p.2494)*
- CWE-937: OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities *(p.2392)*
- CWE-1035: OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities *(p.2439)*
- CWE-1104: Use of Unmaintained Third Party Components *(p.1944)*

CWE-1353: OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures *(p.2494)*
- CWE-255: Credentials Management Errors *(p.2315)*
- CWE-259: Use of Hard-coded Password *(p.623)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
- CWE-290: Authentication Bypass by Spoofing *(p.705)*
- CWE-294: Authentication Bypass by Capture-replay *(p.712)*
- CWE-295: Improper Certificate Validation *(p.714)*
- CWE-297: Improper Validation of Certificate with Host Mismatch *(p.722)*
- CWE-300: Channel Accessible by Non-Endpoint *(p.730)*
- CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
- CWE-304: Missing Critical Step in Authentication *(p.738)*
- CWE-306: Missing Authentication for Critical Function *(p.741)*
- CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
- CWE-346: Origin Validation Error *(p.853)*
- CWE-384: Session Fixation *(p.936)*
- CWE-521: Weak Password Requirements *(p.1223)*
- CWE-613: Insufficient Session Expiration *(p.1371)*
- CWE-620: Unverified Password Change *(p.1383)*
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*
- CWE-1216: Lockout Mechanism Errors *(p.2478)*

CWE-1354: OWASP Top Ten 2021 Category A08:2021 - Software and Data Integrity Failures *(p.2495)*
- CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
- CWE-353: Missing Support for Integrity Check *(p.874)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
- CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision *(p.1653)*
- CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
- CWE-830: Inclusion of Web Functionality from an Untrusted Source *(p.1747)*
- CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes *(p.1809)*

CWE-1355: OWASP Top Ten 2021 Category A09:2021 - Security Logging and Monitoring Failures *(p.2496)*
- CWE-117: Improper Output Neutralization for Logs *(p.288)*

- B CWE-223: Omission of Security-relevant Information *(p.559)*
- B CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
- B CWE-778: Insufficient Logging *(p.1638)*

C CWE-1356: OWASP Top Ten 2021 Category A10:2021 - Server-Side Request Forgery (SSRF) *(p.2497)*

- B CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*

Graph View: CWE-1350: Weaknesses in the 2020 CWE Top 25 Most Dangerous Software Weaknesses

- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
- CWE-416: Use After Free *(p.1012)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-269: Improper Privilege Management *(p.646)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-306: Missing Authentication for Critical Function *(p.741)*
- CWE-862: Missing Authorization *(p.1780)*

Graph View: CWE-1358: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS

- CWE-1359: ICS Communications *(p.2497)*
  - CWE-1364: ICS Communications: Zone Boundary Failures *(p.2501)*
    - CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
    - CWE-268: Privilege Chaining *(p.644)*
    - CWE-269: Improper Privilege Management *(p.646)*
    - CWE-287: Improper Authentication *(p.692)*
    - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
    - CWE-306: Missing Authentication for Critical Function *(p.741)*
    - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
    - CWE-384: Session Fixation *(p.936)*
    - CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
    - CWE-494: Download of Code Without Integrity Check *(p.1185)*
    - CWE-501: Trust Boundary Violation *(p.1203)*
    - CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
    - CWE-669: Incorrect Resource Transfer Between Spheres *(p.1471)*
    - CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
    - CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
    - CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
    - CWE-1263: Improper Physical Access Control *(p.2085)*
    - CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
    - CWE-1393: Use of Default Password *(p.2273)*
  - CWE-1365: ICS Communications: Unreliability *(p.2502)*
    - CWE-121: Stack-based Buffer Overflow *(p.314)*
    - CWE-269: Improper Privilege Management *(p.646)*
    - CWE-306: Missing Authentication for Critical Function *(p.741)*
    - CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
    - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
    - CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
    - CWE-1247: Improper Protection Against Voltage and Clock Glitches *(p.2044)*
    - CWE-1261: Improper Handling of Single Event Upsets *(p.2079)*
    - CWE-1332: Improper Handling of Faults that Lead to Instruction Skips *(p.2227)*
    - CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments *(p.2252)*
    - CWE-1384: Improper Handling of Physical or Environmental Conditions *(p.2257)*
  - CWE-1366: ICS Communications: Frail Security in Protocols *(p.2503)*
    - CWE-121: Stack-based Buffer Overflow *(p.314)*
    - CWE-125: Out-of-bounds Read *(p.330)*
    - CWE-268: Privilege Chaining *(p.644)*
    - CWE-269: Improper Privilege Management *(p.646)*
    - CWE-276: Incorrect Default Permissions *(p.665)*
    - CWE-290: Authentication Bypass by Spoofing *(p.705)*
    - CWE-306: Missing Authentication for Critical Function *(p.741)*
    - CWE-311: Missing Encryption of Sensitive Data *(p.757)*
    - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
    - CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
    - CWE-325: Missing Cryptographic Step *(p.794)*
    - CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
    - CWE-330: Use of Insufficiently Random Values *(p.814)*
    - CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
    - CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*

- CWE-341: Predictable from Observable State *(p.843)*
- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- CWE-358: Improperly Implemented Security Check for Standard *(p.881)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-377: Insecure Temporary File *(p.925)*
- CWE-384: Session Fixation *(p.936)*
- CWE-648: Incorrect Use of Privileged APIs *(p.1428)*
- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
- CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
- CWE-1393: Use of Default Password *(p.2273)*

CWE-1360: ICS Dependencies (& Architecture) *(p.2498)*

- CWE-1367: ICS Dependencies (& Architecture): External Physical Systems *(p.2504)*
  - CWE-1247: Improper Protection Against Voltage and Clock Glitches *(p.2044)*
  - CWE-1338: Improper Protections Against Hardware Overheating *(p.2240)*
  - CWE-1357: Reliance on Insufficiently Trustworthy Component *(p.2254)*
  - CWE-1384: Improper Handling of Physical or Environmental Conditions *(p.2257)*
- CWE-1368: ICS Dependencies (& Architecture): External Digital Systems *(p.2505)*
  - CWE-15: External Control of System or Configuration Setting *(p.17)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-306: Missing Authentication for Critical Function *(p.741)*
  - CWE-308: Use of Single-factor Authentication *(p.752)*
  - CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
  - CWE-440: Expected Behavior Violation *(p.1062)*
  - CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
  - CWE-603: Use of Client-Side Authentication *(p.1354)*
  - CWE-610: Externally Controlled Reference to a Resource in Another Sphere *(p.1364)*
  - CWE-638: Not Using Complete Mediation *(p.1404)*
  - CWE-1059: Insufficient Technical Documentation *(p.1894)*
  - CWE-1068: Inconsistency Between Implementation and Documented Design *(p.1906)*
  - CWE-1104: Use of Unmaintained Third Party Components *(p.1944)*
  - CWE-1329: Reliance on Component That is Not Updateable *(p.2219)*
  - CWE-1357: Reliance on Insufficiently Trustworthy Component *(p.2254)*
  - CWE-1393: Use of Default Password *(p.2273)*

CWE-1361: ICS Supply Chain *(p.2499)*

- CWE-1369: ICS Supply Chain: IT/OT Convergence/Expansion *(p.2506)*
  - CWE-636: Not Failing Securely ('Failing Open') *(p.1401)*
  - CWE-284: Improper Access Control *(p.680)*
- CWE-1370: ICS Supply Chain: Common Mode Frailties *(p.2507)*
  - CWE-664: Improper Control of a Resource Through its Lifetime *(p.1454)*
  - CWE-707: Improper Neutralization *(p.1546)*
  - CWE-710: Improper Adherence to Coding Standards *(p.1549)*
  - CWE-1357: Reliance on Insufficiently Trustworthy Component *(p.2254)*
  - CWE-329: Generation of Predictable IV with CBC Mode *(p.811)*
  - CWE-693: Protection Mechanism Failure *(p.1520)*
- CWE-1371: ICS Supply Chain: Poorly Documented or Undocumented Features *(p.2508)*
  - CWE-489: Active Debug Code *(p.1171)*
  - CWE-912: Hidden Functionality *(p.1803)*
  - CWE-1059: Insufficient Technical Documentation *(p.1894)*
  - CWE-1242: Inclusion of Undocumented Features or Chicken Bits *(p.2033)*
- CWE-1372: ICS Supply Chain: OT Counterfeit and Malicious Corruption *(p.2509)*
  - CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques *(p.2118)*

- CWE-1198: Privilege Separation and Access Control Issues *(p.2470)*
- CWE-1231: Improper Prevention of Lock Bit Modification *(p.2007)*
- CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2012)*
- CWE-284: Improper Access Control *(p.680)*

CWE-1362: ICS Engineering (Constructions/Deployment) *(p.2499)*
- CWE-1373: ICS Engineering (Construction/Deployment): Trust Model Problems *(p.2510)*
  - CWE-269: Improper Privilege Management *(p.646)*
  - CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
  - CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- CWE-1374: ICS Engineering (Construction/Deployment): Maker Breaker Blindness *(p.2510)*
- CWE-1375: ICS Engineering (Construction/Deployment): Gaps in Details/Data *(p.2511)*
  - CWE-1059: Insufficient Technical Documentation *(p.1894)*
  - CWE-1110: Incomplete Design Documentation *(p.1950)*
  - CWE-710: Improper Adherence to Coding Standards *(p.1549)*
  - CWE-1053: Missing Documentation for Design *(p.1888)*
  - CWE-1111: Incomplete I/O Documentation *(p.1951)*
- CWE-1376: ICS Engineering (Construction/Deployment): Security Gaps in Commissioning *(p.2512)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
  - CWE-1393: Use of Default Password *(p.2273)*
- CWE-1377: ICS Engineering (Construction/Deployment): Inherent Predictability in Design *(p.2513)*
  - CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques *(p.2118)*

CWE-1363: ICS Operations (& Maintenance) *(p.2500)*
- CWE-1378: ICS Operations (& Maintenance): Gaps in obligations and training *(p.2513)*
- CWE-1379: ICS Operations (& Maintenance): Human factors in ICS environments *(p.2514)*
  - CWE-655: Insufficient Psychological Acceptability *(p.1442)*
  - CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1079)*
- CWE-1380: ICS Operations (& Maintenance): Post-analysis changes *(p.2515)*
- CWE-1381: ICS Operations (& Maintenance): Exploitable Standard Operational Procedures *(p.2516)*
- CWE-1382: ICS Operations (& Maintenance): Emerging Energy Technologies *(p.2517)*
  - CWE-20: Improper Input Validation *(p.20)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-295: Improper Certificate Validation *(p.714)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
  - CWE-346: Origin Validation Error *(p.853)*
  - CWE-406: Insufficient Control of Network Message Volume (Network Amplification) *(p.990)*
  - CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
- CWE-1383: ICS Operations (& Maintenance): Compliance/Conformance with Regulatory Requirements *(p.2517)*
  - CWE-710: Improper Adherence to Coding Standards *(p.1549)*

Graph View: CWE-1387: Weaknesses in the 2022 CWE Top 25 Most Dangerous Software Weaknesses

- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-416: Use After Free *(p.1012)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-862: Missing Authorization *(p.1780)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
- CWE-306: Missing Authentication for Critical Function *(p.741)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-276: Incorrect Default Permissions *(p.665)*
- CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*

Graph View: CWE-1400: Comprehensive Categorization for Software Assurance Trends

- CWE-1396: Comprehensive Categorization: Access Control *(p.2519)*
  - CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods *(p.8)*
  - CWE-13: ASP.NET Misconfiguration: Password in Configuration File *(p.13)*
  - CWE-202: Exposure of Sensitive Information Through Data Queries *(p.516)*
  - CWE-256: Plaintext Storage of a Password *(p.615)*
  - CWE-257: Storing Passwords in a Recoverable Format *(p.618)*
  - CWE-258: Empty Password in Configuration File *(p.621)*
  - CWE-259: Use of Hard-coded Password *(p.623)*
  - CWE-260: Password in Configuration File *(p.629)*
  - CWE-261: Weak Encoding for Password *(p.631)*
  - CWE-262: Not Using Password Aging *(p.633)*
  - CWE-263: Password Aging with Long Expiration *(p.636)*
  - CWE-266: Incorrect Privilege Assignment *(p.638)*
  - CWE-267: Privilege Defined With Unsafe Actions *(p.641)*
  - CWE-268: Privilege Chaining *(p.644)*
  - CWE-269: Improper Privilege Management *(p.646)*
  - CWE-270: Privilege Context Switching Error *(p.651)*
  - CWE-271: Privilege Dropping / Lowering Errors *(p.653)*
  - CWE-272: Least Privilege Violation *(p.656)*
  - CWE-273: Improper Check for Dropped Privileges *(p.660)*
  - CWE-274: Improper Handling of Insufficient Privileges *(p.663)*
  - CWE-276: Incorrect Default Permissions *(p.665)*
  - CWE-277: Insecure Inherited Permissions *(p.668)*
  - CWE-278: Insecure Preserved Inherited Permissions *(p.669)*
  - CWE-279: Incorrect Execution-Assigned Permissions *(p.671)*
  - CWE-280: Improper Handling of Insufficient Permissions or Privileges *(p.672)*
  - CWE-281: Improper Preservation of Permissions *(p.674)*
  - CWE-282: Improper Ownership Management *(p.676)*
  - CWE-283: Unverified Ownership *(p.678)*
  - CWE-284: Improper Access Control *(p.680)*
  - CWE-285: Improper Authorization *(p.684)*
  - CWE-286: Incorrect User Management *(p.691)*
  - CWE-287: Improper Authentication *(p.692)*
  - CWE-288: Authentication Bypass Using an Alternate Path or Channel *(p.700)*
  - CWE-289: Authentication Bypass by Alternate Name *(p.703)*
  - CWE-290: Authentication Bypass by Spoofing *(p.705)*
  - CWE-291: Reliance on IP Address for Authentication *(p.708)*
  - CWE-293: Using Referer Field for Authentication *(p.710)*
  - CWE-294: Authentication Bypass by Capture-replay *(p.712)*
  - CWE-295: Improper Certificate Validation *(p.714)*
  - CWE-296: Improper Following of a Certificate's Chain of Trust *(p.719)*
  - CWE-297: Improper Validation of Certificate with Host Mismatch *(p.722)*
  - CWE-298: Improper Validation of Certificate Expiration *(p.726)*
  - CWE-299: Improper Check for Certificate Revocation *(p.727)*
  - CWE-300: Channel Accessible by Non-Endpoint *(p.730)*
  - CWE-301: Reflection Attack in an Authentication Protocol *(p.733)*
  - CWE-302: Authentication Bypass by Assumed-Immutable Data *(p.735)*
  - CWE-303: Incorrect Implementation of Authentication Algorithm *(p.737)*
  - CWE-304: Missing Critical Step in Authentication *(p.738)*
  - CWE-305: Authentication Bypass by Primary Weakness *(p.740)*

- CWE-306: Missing Authentication for Critical Function *(p.741)*
- CWE-307: Improper Restriction of Excessive Authentication Attempts *(p.747)*
- CWE-308: Use of Single-factor Authentication *(p.752)*
- CWE-309: Use of Password System for Primary Authentication *(p.754)*
- CWE-321: Use of Hard-coded Cryptographic Key *(p.785)*
- CWE-322: Key Exchange without Entity Authentication *(p.788)*
- CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action *(p.863)*
- CWE-370: Missing Check for Certificate Revocation after Initial Check *(p.917)*
- CWE-384: Session Fixation *(p.936)*
- CWE-419: Unprotected Primary Channel *(p.1017)*
- CWE-420: Unprotected Alternate Channel *(p.1018)*
- CWE-421: Race Condition During Access to Alternate Channel *(p.1020)*
- CWE-422: Unprotected Windows Messaging Channel ('Shatter') *(p.1022)*
- CWE-425: Direct Request ('Forced Browsing') *(p.1025)*
- CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') *(p.1064)*
- CWE-520: .NET Misconfiguration: Use of Impersonation *(p.1222)*
- CWE-521: Weak Password Requirements *(p.1223)*
- CWE-522: Insufficiently Protected Credentials *(p.1225)*
- CWE-523: Unprotected Transport of Credentials *(p.1230)*
- CWE-549: Missing Password Field Masking *(p.1262)*
- CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization *(p.1264)*
- CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File *(p.1270)*
- CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation *(p.1271)*
- CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key *(p.1286)*
- CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created *(p.1331)*
- CWE-599: Missing Validation of OpenSSL Certificate *(p.1341)*
- CWE-601: URL Redirection to Untrusted Site ('Open Redirect') *(p.1345)*
- CWE-603: Use of Client-Side Authentication *(p.1354)*
- CWE-611: Improper Restriction of XML External Entity Reference *(p.1367)*
- CWE-612: Improper Authorization of Index Containing Sensitive Information *(p.1370)*
- CWE-613: Insufficient Session Expiration *(p.1371)*
- CWE-620: Unverified Password Change *(p.1383)*
- CWE-623: Unsafe ActiveX Control Marked Safe For Scripting *(p.1389)*
- CWE-639: Authorization Bypass Through User-Controlled Key *(p.1406)*
- CWE-640: Weak Password Recovery Mechanism for Forgotten Password *(p.1409)*
- CWE-645: Overly Restrictive Account Lockout Mechanism *(p.1423)*
- CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions *(p.1426)*
- CWE-648: Incorrect Use of Privileged APIs *(p.1428)*
- CWE-708: Incorrect Ownership Assignment *(p.1548)*
- CWE-732: Incorrect Permission Assignment for Critical Resource *(p.1551)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-804: Guessable CAPTCHA *(p.1701)*
- CWE-836: Use of Password Hash Instead of Password for Authentication *(p.1761)*
- CWE-842: Placement of User into Incorrect Group *(p.1775)*
- CWE-862: Missing Authorization *(p.1780)*
- CWE-863: Incorrect Authorization *(p.1787)*
- CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*
- CWE-921: Storage of Sensitive Data in a Mechanism without Access Control *(p.1824)*
- CWE-923: Improper Restriction of Communication Channel to Intended Endpoints *(p.1827)*
- CWE-925: Improper Verification of Intent by Broadcast Receiver *(p.1831)*
- CWE-926: Improper Export of Android Application Components *(p.1833)*
- CWE-927: Use of Implicit Intent for Sensitive Communication *(p.1836)*
- CWE-939: Improper Authorization in Handler for Custom URL Scheme *(p.1840)*

- CWE-940: Improper Verification of Source of a Communication Channel *(p.1842)*
- CWE-941: Incorrectly Specified Destination in a Communication Channel *(p.1845)*
- CWE-942: Permissive Cross-domain Policy with Untrusted Domains *(p.1847)*
- CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag *(p.1854)*
- CWE-1021: Improper Restriction of Rendered UI Layers or Frames *(p.1860)*
- CWE-1022: Use of Web Link to Untrusted Target with window.opener Access *(p.1862)*
- CWE-1191: On-Chip Debug and Test Interface With Improper Access Control *(p.1980)*
- CWE-1220: Insufficient Granularity of Access Control *(p.1992)*
- CWE-1222: Insufficient Granularity of Address Regions Protected by Register Locks *(p.1999)*
- CWE-1224: Improper Restriction of Write-Once Bit Fields *(p.2003)*
- CWE-1230: Exposure of Sensitive Information Through Metadata *(p.2006)*
- CWE-1231: Improper Prevention of Lock Bit Modification *(p.2007)*
- CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection *(p.2012)*
- CWE-1242: Inclusion of Undocumented Features or Chicken Bits *(p.2033)*
- CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug *(p.2035)*
- CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State *(p.2037)*
- CWE-1252: CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations *(p.2056)*
- CWE-1256: Improper Restriction of Software Interfaces to Hardware Features *(p.2065)*
- CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions *(p.2068)*
- CWE-1259: Improper Restriction of Security Token Assignment *(p.2073)*
- CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges *(p.2075)*
- CWE-1262: Improper Access Control for Register Interface *(p.2081)*
- CWE-1263: Improper Physical Access Control *(p.2085)*
- CWE-1267: Policy Uses Obsolete Encoding *(p.2093)*
- CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents *(p.2095)*
- CWE-1270: Generation of Incorrect Security Tokens *(p.2100)*
- CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code *(p.2108)*
- CWE-1275: Sensitive Cookie with Improper SameSite Attribute *(p.2110)*
- CWE-1276: Hardware Child Block Incorrectly Connected to Parent System *(p.2113)*
- CWE-1283: Mutable Attestation or Measurement Reporting Data *(p.2128)*
- CWE-1290: Incorrect Decoding of Security Identifiers *(p.2142)*
- CWE-1292: Incorrect Conversion of Security Identifiers *(p.2147)*
- CWE-1294: Insecure Security Identifier Mechanism *(p.2150)*
- CWE-1296: Incorrect Chaining or Granularity of Debug Components *(p.2153)*
- CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT Vendors *(p.2156)*
- CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface *(p.2162)*
- CWE-1302: Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC) *(p.2172)*
- CWE-1304: Improperly Preserved Integrity of Hardware Configuration State During a Power Save/ Restore Operation *(p.2176)*
- CWE-1311: Improper Translation of Security Attributes by Fabric Bridge *(p.2182)*
- CWE-1312: Missing Protection for Mirrored Regions in On-Chip Fabric Firewall *(p.2184)*
- CWE-1313: Hardware Allows Activation of Test or Debug Logic at Runtime *(p.2185)*
- CWE-1314: Missing Write Protection for Parametric Data Values *(p.2187)*
- CWE-1315: Improper Setting of Bus Controlling Capability in Fabric End-point *(p.2190)*
- CWE-1316: Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges *(p.2192)*
- CWE-1317: Improper Access Control in Fabric Bridge *(p.2194)*
- CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals *(p.2202)*
- CWE-1323: Improper Management of Sensitive Trace Data *(p.2208)*
- CWE-1328: Security Version Number Mutable to Older Versions *(p.2217)*
- CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy *(p.2234)*
- CWE-1390: Weak Authentication *(p.2267)*

- CWE-1391: Use of Weak Credentials *(p.2269)*
- CWE-1392: Use of Default Credentials *(p.2271)*
- CWE-1393: Use of Default Password *(p.2273)*
- CWE-1394: Use of Default Cryptographic Key *(p.2275)*

CWE-1397: Comprehensive Categorization: Comparison *(p.2523)*
- CWE-183: Permissive List of Allowed Inputs *(p.458)*
- CWE-185: Incorrect Regular Expression *(p.463)*
- CWE-186: Overly Restrictive Regular Expression *(p.466)*
- CWE-187: Partial String Comparison *(p.467)*
- CWE-478: Missing Default Case in Multiple Condition Expression *(p.1142)*
- CWE-486: Comparison of Classes by Name *(p.1164)*
- CWE-595: Comparison of Object References Instead of Object Contents *(p.1334)*
- CWE-597: Use of Wrong Operator in String Comparison *(p.1337)*
- CWE-625: Permissive Regular Expression *(p.1392)*
- CWE-697: Incorrect Comparison *(p.1530)*
- CWE-777: Regular Expression without Anchors *(p.1636)*
- CWE-839: Numeric Range Comparison Without Minimum Check *(p.1767)*
- CWE-1023: Incomplete Comparison with Missing Factors *(p.1865)*
- CWE-1024: Comparison of Incompatible Types *(p.1867)*
- CWE-1025: Comparison Using Wrong Factors *(p.1868)*
- CWE-1077: Floating Point Comparison with Incorrect Operator *(p.1917)*

CWE-1398: Comprehensive Categorization: Component Interaction *(p.2524)*
- CWE-14: Compiler Removal of Code to Clear Buffers *(p.14)*
- CWE-115: Misinterpretation of Input *(p.280)*
- CWE-435: Improper Interaction Between Multiple Correctly-Behaving Entities *(p.1055)*
- CWE-436: Interpretation Conflict *(p.1057)*
- CWE-437: Incomplete Model of Endpoint Features *(p.1059)*
- CWE-439: Behavioral Change in New Version or Environment *(p.1061)*
- CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') *(p.1068)*
- CWE-650: Trusting HTTP Permission Methods on the Server Side *(p.1432)*
- CWE-733: Compiler Optimization Removal or Modification of Security-critical Code *(p.1562)*
- CWE-1037: Processor Optimization Removal or Modification of Security-critical Code *(p.1870)*
- CWE-1038: Insecure Automated Optimizations *(p.1872)*

CWE-1401: Comprehensive Categorization: Concurrency *(p.2526)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-363: Race Condition Enabling Link Following *(p.897)*
- CWE-364: Signal Handler Race Condition *(p.899)*
- CWE-366: Race Condition within a Thread *(p.904)*
- CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition *(p.906)*
- CWE-368: Context Switching Race Condition *(p.912)*
- CWE-412: Unrestricted Externally Accessible Lock *(p.1000)*
- CWE-413: Improper Resource Locking *(p.1003)*
- CWE-414: Missing Lock Check *(p.1007)*
- CWE-432: Dangerous Signal Handler not Disabled During Sensitive Operations *(p.1045)*
- CWE-479: Signal Handler Use of a Non-reentrant Function *(p.1147)*
- CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context *(p.1255)*
- CWE-558: Use of getlogin() in Multithreaded Application *(p.1272)*
- CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context *(p.1288)*
- CWE-572: Call to Thread run() instead of start() *(p.1296)*
- CWE-574: EJB Bad Practices: Use of Synchronization Primitives *(p.1300)*
- CWE-591: Sensitive Data Storage in Improperly Locked Memory *(p.1329)*
- CWE-609: Double-Checked Locking *(p.1362)*

- CWE-663: Use of a Non-reentrant Function in a Concurrent Context *(p.1452)*
- CWE-667: Improper Locking *(p.1464)*
- CWE-689: Permission Race Condition During Resource Copy *(p.1513)*
- CWE-764: Multiple Locks of a Critical Resource *(p.1604)*
- CWE-765: Multiple Unlocks of a Critical Resource *(p.1605)*
- CWE-820: Missing Synchronization *(p.1720)*
- CWE-821: Incorrect Synchronization *(p.1722)*
- CWE-828: Signal Handler with Functionality that is not Asynchronous-Safe *(p.1737)*
- CWE-831: Signal Handler Function Associated with Multiple Signals *(p.1749)*
- CWE-832: Unlock of a Resource that is not Locked *(p.1752)*
- CWE-833: Deadlock *(p.1753)*
- CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element *(p.1893)*
- CWE-1088: Synchronous Access of Remote Resource without Timeout *(p.1928)*
- CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization *(p.1936)*
- CWE-1223: Race Condition for Write-Once Attributes *(p.2001)*
- CWE-1232: Improper Lock Behavior After Power State Transition *(p.2010)*
- CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks *(p.2014)*
- CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels *(p.2086)*
- CWE-1298: Hardware Logic Contains Race Conditions *(p.2158)*

CWE-1402: Comprehensive Categorization: Encryption *(p.2527)*

- CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption *(p.1)*
- CWE-311: Missing Encryption of Sensitive Data *(p.757)*
- CWE-312: Cleartext Storage of Sensitive Information *(p.764)*
- CWE-313: Cleartext Storage in a File or on Disk *(p.770)*
- CWE-314: Cleartext Storage in the Registry *(p.772)*
- CWE-315: Cleartext Storage of Sensitive Information in a Cookie *(p.774)*
- CWE-316: Cleartext Storage of Sensitive Information in Memory *(p.775)*
- CWE-317: Cleartext Storage of Sensitive Information in GUI *(p.777)*
- CWE-318: Cleartext Storage of Sensitive Information in Executable *(p.778)*
- CWE-319: Cleartext Transmission of Sensitive Information *(p.779)*
- CWE-324: Use of a Key Past its Expiration Date *(p.792)*
- CWE-325: Missing Cryptographic Step *(p.794)*
- CWE-326: Inadequate Encryption Strength *(p.796)*
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm *(p.799)*
- CWE-328: Use of Weak Hash *(p.806)*
- CWE-347: Improper Verification of Cryptographic Signature *(p.857)*
- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute *(p.1373)*
- CWE-759: Use of a One-Way Hash without a Salt *(p.1585)*
- CWE-760: Use of a One-Way Hash with a Predictable Salt *(p.1589)*
- CWE-780: Use of RSA Algorithm without OAEP *(p.1644)*
- CWE-916: Use of Password Hash With Insufficient Computational Effort *(p.1813)*
- CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation *(p.2025)*

CWE-1403: Comprehensive Categorization: Exposed Resource *(p.2528)*

- CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote *(p.6)*
- CWE-15: External Control of System or Configuration Setting *(p.17)*
- CWE-73: External Control of File Name or Path *(p.132)*
- CWE-114: Process Control *(p.277)*
- CWE-219: Storage of File with Sensitive Data Under Web Root *(p.553)*
- CWE-220: Storage of File With Sensitive Data Under FTP Root *(p.555)*
- CWE-374: Passing Mutable Objects to an Untrusted Method *(p.920)*
- CWE-375: Returning a Mutable Object to an Untrusted Caller *(p.923)*
- CWE-377: Insecure Temporary File *(p.925)*

- CWE-378: Creation of Temporary File With Insecure Permissions *(p.928)*
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions *(p.930)*
- CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') *(p.976)*
- CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') *(p.978)*
- CWE-426: Untrusted Search Path *(p.1028)*
- CWE-427: Uncontrolled Search Path Element *(p.1033)*
- CWE-428: Unquoted Search Path or Element *(p.1039)*
- CWE-433: Unparsed Raw Web Content Delivery *(p.1046)*
- CWE-472: External Control of Assumed-Immutable Web Parameter *(p.1123)*
- CWE-488: Exposure of Data Element to Wrong Session *(p.1169)*
- CWE-491: Public cloneable() Method Without Final ('Object Hijack') *(p.1174)*
- CWE-492: Use of Inner Class Containing Sensitive Data *(p.1175)*
- CWE-493: Critical Public Variable Without Final Modifier *(p.1182)*
- CWE-498: Cloneable Class Containing Sensitive Information *(p.1196)*
- CWE-499: Serializable Class Containing Sensitive Data *(p.1198)*
- CWE-500: Public Static Field Not Marked Final *(p.1200)*
- CWE-524: Use of Cache Containing Sensitive Information *(p.1232)*
- CWE-525: Use of Web Browser Cache Containing Sensitive Information *(p.1233)*
- CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere *(p.1236)*
- CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere *(p.1237)*
- CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere *(p.1238)*
- CWE-530: Exposure of Backup File to an Unauthorized Control Sphere *(p.1239)*
- CWE-539: Use of Persistent Cookies Containing Sensitive Information *(p.1250)*
- CWE-552: Files or Directories Accessible to External Parties *(p.1265)*
- CWE-553: Command Shell in Externally Accessible Directory *(p.1269)*
- CWE-565: Reliance on Cookies without Validation and Integrity Checking *(p.1283)*
- CWE-582: Array Declared Public, Final, and Static *(p.1314)*
- CWE-583: finalize() Method Declared Public *(p.1315)*
- CWE-608: Struts: Non-private Field in ActionForm Class *(p.1361)*
- CWE-619: Dangling Database Cursor ('Cursor Injection') *(p.1382)*
- CWE-642: External Control of Critical State Data *(p.1414)*
- CWE-668: Exposure of Resource to Wrong Sphere *(p.1469)*
- CWE-767: Access to Critical Private Variable via Public Method *(p.1610)*
- CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision *(p.1653)*
- CWE-1282: Assumed-Immutable Data is Stored in Writable Memory *(p.2127)*
- CWE-1327: Binding to an Unrestricted IP Address *(p.2215)*

CWE-1404: Comprehensive Categorization: File Handling *(p.2529)*

- 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.54)*
- CWE-26: Path Traversal: '/dir/../filename' *(p.56)*
- CWE-27: Path Traversal: 'dir/../../filename' *(p.58)*
- CWE-28: Path Traversal: '..\filedir' *(p.59)*
- CWE-29: Path Traversal: '\..\filename' *(p.61)*
- CWE-30: Path Traversal: '\dir\..\filename' *(p.63)*
- 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.80)*
- CWE-39: Path Traversal: 'C:dirname' *(p.82)*
- CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) *(p.85)*
- CWE-41: Improper Resolution of Path Equivalence *(p.86)*
- CWE-42: Path Equivalence: 'filename.' (Trailing Dot) *(p.92)*
- CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) *(p.93)*
- CWE-44: Path Equivalence: 'file.name' (Internal Dot) *(p.94)*
- CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) *(p.95)*
- CWE-46: Path Equivalence: 'filename ' (Trailing Space) *(p.96)*
- CWE-47: Path Equivalence: ' filename' (Leading Space) *(p.97)*
- CWE-48: Path Equivalence: 'file name' (Internal Whitespace) *(p.98)*
- CWE-49: Path Equivalence: 'filename/' (Trailing Slash) *(p.99)*
- CWE-50: Path Equivalence: '//multiple/leading/slash' *(p.100)*
- CWE-51: Path Equivalence: '/multiple//internal/slash' *(p.102)*
- CWE-52: Path Equivalence: '/multiple/trailing/slash//' *(p.103)*
- CWE-53: Path Equivalence: '\multiple\\internal\backslash' *(p.104)*
- CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) *(p.105)*
- CWE-55: Path Equivalence: '/./' (Single Dot Directory) *(p.106)*
- CWE-56: Path Equivalence: 'filedir*' (Wildcard) *(p.107)*
- CWE-57: Path Equivalence: 'fakedir/../realdir/filename' *(p.108)*
- CWE-58: Path Equivalence: Windows 8.3 Filename *(p.110)*
- CWE-59: Improper Link Resolution Before File Access ('Link Following') *(p.111)*
- CWE-61: UNIX Symbolic Link (Symlink) Following *(p.116)*
- CWE-62: UNIX Hard Link *(p.119)*
- CWE-64: Windows Shortcut Following (.LNK) *(p.121)*
- CWE-65: Windows Hard Link *(p.123)*
- CWE-66: Improper Handling of File Names that Identify Virtual Resources *(p.124)*
- CWE-67: Improper Handling of Windows Device Names *(p.126)*
- CWE-69: Improper Handling of Windows ::DATA Alternate Data Stream *(p.129)*
- CWE-72: Improper Handling of Apple HFS+ Alternate Data Stream Path *(p.130)*

CWE-1405: Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions *(p.2531)*

- CWE-7: J2EE Misconfiguration: Missing Custom Error Page *(p.4)*
- CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page *(p.11)*
- CWE-252: Unchecked Return Value *(p.606)*
- CWE-390: Detection of Error Condition Without Action *(p.943)*
- CWE-391: Unchecked Error Condition *(p.948)*
- CWE-394: Unexpected Status Code or Return Value *(p.955)*
- CWE-544: Missing Standardized Error Handling Mechanism *(p.1256)*
- CWE-703: Improper Check or Handling of Exceptional Conditions *(p.1535)*
- CWE-754: Improper Check for Unusual or Exceptional Conditions *(p.1568)*
- CWE-755: Improper Handling of Exceptional Conditions *(p.1576)*
- CWE-756: Missing Custom Error Page *(p.1579)*
- CWE-1247: Improper Protection Against Voltage and Clock Glitches *(p.2044)*
- CWE-1261: Improper Handling of Single Event Upsets *(p.2079)*
- CWE-1332: Improper Handling of Faults that Lead to Instruction Skips *(p.2227)*
- CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments *(p.2252)*
- CWE-1384: Improper Handling of Physical or Environmental Conditions *(p.2257)*

CWE-1406: Comprehensive Categorization: Improper Input Validation *(p.2531)*

- CWE-20: Improper Input Validation *(p.20)*
- CWE-105: Struts: Form Field Without Validator *(p.253)*
- CWE-106: Struts: Plug-in Framework not in Use *(p.256)*
- CWE-108: Struts: Unvalidated Action Form *(p.261)*
- CWE-109: Struts: Validator Turned Off *(p.263)*

- CWE-112: Missing XML Validation *(p.269)*
- CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework *(p.1269)*
- CWE-606: Unchecked Input for Loop Condition *(p.1357)*
- CWE-622: Improper Validation of Function Hook Arguments *(p.1387)*
- CWE-781: Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code *(p.1646)*
- CWE-1173: Improper Use of Validation Framework *(p.1969)*
- CWE-1174: ASP.NET Misconfiguration: Improper Model Validation *(p.1970)*
- CWE-1284: Improper Validation of Specified Quantity in Input *(p.2130)*
- CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input *(p.2132)*
- CWE-1286: Improper Validation of Syntactic Correctness of Input *(p.2136)*
- CWE-1287: Improper Validation of Specified Type of Input *(p.2138)*
- CWE-1288: Improper Validation of Consistency within Input *(p.2139)*
- CWE-1289: Improper Validation of Unsafe Equivalence in Input *(p.2141)*

CWE-1407: Comprehensive Categorization: Improper Neutralization *(p.2532)*

- CWE-116: Improper Encoding or Escaping of Output *(p.281)*
- CWE-117: Improper Output Neutralization for Logs *(p.288)*
- CWE-130: Improper Handling of Length Parameter Inconsistency *(p.351)*
- CWE-138: Improper Neutralization of Special Elements *(p.373)*
- CWE-140: Improper Neutralization of Delimiters *(p.376)*
- CWE-141: Improper Neutralization of Parameter/Argument Delimiters *(p.378)*
- CWE-142: Improper Neutralization of Value Delimiters *(p.380)*
- CWE-143: Improper Neutralization of Record Delimiters *(p.381)*
- CWE-144: Improper Neutralization of Line Delimiters *(p.383)*
- CWE-145: Improper Neutralization of Section Delimiters *(p.385)*
- CWE-146: Improper Neutralization of Expression/Command Delimiters *(p.387)*
- CWE-147: Improper Neutralization of Input Terminators *(p.389)*
- CWE-148: Improper Neutralization of Input Leaders *(p.391)*
- CWE-149: Improper Neutralization of Quoting Syntax *(p.392)*
- CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences *(p.394)*
- CWE-151: Improper Neutralization of Comment Delimiters *(p.396)*
- CWE-152: Improper Neutralization of Macro Symbols *(p.398)*
- CWE-153: Improper Neutralization of Substitution Characters *(p.400)*
- CWE-154: Improper Neutralization of Variable Name Delimiters *(p.401)*
- CWE-155: Improper Neutralization of Wildcards or Matching Symbols *(p.403)*
- CWE-156: Improper Neutralization of Whitespace *(p.405)*
- CWE-157: Failure to Sanitize Paired Delimiters *(p.407)*
- CWE-158: Improper Neutralization of Null Byte or NUL Character *(p.409)*
- CWE-159: Improper Handling of Invalid Use of Special Elements *(p.411)*
- CWE-160: Improper Neutralization of Leading Special Elements *(p.413)*
- CWE-161: Improper Neutralization of Multiple Leading Special Elements *(p.415)*
- CWE-162: Improper Neutralization of Trailing Special Elements *(p.417)*
- CWE-163: Improper Neutralization of Multiple Trailing Special Elements *(p.418)*
- CWE-164: Improper Neutralization of Internal Special Elements *(p.420)*
- CWE-165: Improper Neutralization of Multiple Internal Special Elements *(p.422)*
- CWE-166: Improper Handling of Missing Special Element *(p.423)*
- CWE-167: Improper Handling of Additional Special Element *(p.425)*
- CWE-168: Improper Handling of Inconsistent Special Elements *(p.426)*
- CWE-170: Improper Null Termination *(p.428)*
- CWE-172: Encoding Error *(p.433)*
- CWE-173: Improper Handling of Alternate Encoding *(p.435)*
- CWE-174: Double Decoding of the Same Data *(p.437)*
- CWE-175: Improper Handling of Mixed Encoding *(p.439)*
- CWE-176: Improper Handling of Unicode Encoding *(p.440)*
- CWE-177: Improper Handling of URL Encoding (Hex Encoding) *(p.442)*

- CWE-228: Improper Handling of Syntactically Invalid Structure *(p.568)*
- CWE-229: Improper Handling of Values *(p.570)*
- CWE-230: Improper Handling of Missing Values *(p.570)*
- CWE-231: Improper Handling of Extra Values *(p.572)*
- CWE-232: Improper Handling of Undefined Values *(p.573)*
- CWE-233: Improper Handling of Parameters *(p.574)*
- CWE-234: Failure to Handle Missing Parameter *(p.576)*
- CWE-235: Improper Handling of Extra Parameters *(p.578)*
- CWE-236: Improper Handling of Undefined Parameters *(p.579)*
- CWE-237: Improper Handling of Structural Elements *(p.580)*
- CWE-238: Improper Handling of Incomplete Structural Elements *(p.581)*
- CWE-239: Failure to Handle Incomplete Element *(p.582)*
- CWE-240: Improper Handling of Inconsistent Structural Elements *(p.583)*
- CWE-241: Improper Handling of Unexpected Data Type *(p.584)*
- CWE-463: Deletion of Data Structure Sentinel *(p.1105)*
- CWE-464: Addition of Data Structure Sentinel *(p.1107)*
- CWE-626: Null Byte Interaction Error (Poison Null Byte) *(p.1394)*
- CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax *(p.1422)*
- CWE-707: Improper Neutralization *(p.1546)*
- CWE-790: Improper Filtering of Special Elements *(p.1678)*
- CWE-791: Incomplete Filtering of Special Elements *(p.1680)*
- CWE-792: Incomplete Filtering of One or More Instances of Special Elements *(p.1681)*
- CWE-793: Only Filtering One Instance of a Special Element *(p.1683)*
- CWE-794: Incomplete Filtering of Multiple Instances of Special Elements *(p.1684)*
- CWE-795: Only Filtering Special Elements at a Specified Location *(p.1685)*
- CWE-796: Only Filtering Special Elements Relative to a Marker *(p.1687)*
- CWE-797: Only Filtering Special Elements at an Absolute Position *(p.1689)*
- CWE-838: Inappropriate Encoding for Output Context *(p.1764)*

CWE-1408: Comprehensive Categorization: Incorrect Calculation *(p.2534)*

- CWE-128: Wrap-around Error *(p.339)*
- CWE-135: Incorrect Calculation of Multi-Byte String Length *(p.370)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-191: Integer Underflow (Wrap or Wraparound) *(p.480)*
- CWE-193: Off-by-one Error *(p.486)*
- CWE-369: Divide By Zero *(p.913)*
- CWE-467: Use of sizeof() on a Pointer Type *(p.1110)*
- CWE-468: Incorrect Pointer Scaling *(p.1114)*
- CWE-469: Use of Pointer Subtraction to Determine Size *(p.1115)*
- CWE-682: Incorrect Calculation *(p.1499)*
- CWE-1335: Incorrect Bitwise Shift of Integer *(p.2235)*
- CWE-1339: Insufficient Precision or Accuracy of a Real Number *(p.2242)*

CWE-1409: Comprehensive Categorization: Injection *(p.2535)*

- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') *(p.137)*
- CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) *(p.142)*
- CWE-76: Improper Neutralization of Equivalent Special Elements *(p.144)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) *(p.177)*
- CWE-81: Improper Neutralization of Script in an Error Message Web Page *(p.179)*
- CWE-82: Improper Neutralization of Script in Attributes of IMG Tags in a Web Page *(p.182)*

- CWE-83: Improper Neutralization of Script in Attributes in a Web Page *(p.183)*
- CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page *(p.186)*
- CWE-85: Doubled Character XSS Manipulations *(p.188)*
- CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages *(p.190)*
- CWE-87: Improper Neutralization of Alternate XSS Syntax *(p.192)*
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') *(p.194)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') *(p.212)*
- CWE-91: XML Injection (aka Blind XPath Injection) *(p.215)*
- CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') *(p.217)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') *(p.226)*
- CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') *(p.232)*
- CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page *(p.235)*
- CWE-99: Improper Control of Resource Identifiers ('Resource Injection') *(p.243)*
- CWE-102: Struts: Duplicate Validation Forms *(p.246)*
- CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') *(p.271)*
- CWE-564: SQL Injection: Hibernate *(p.1282)*
- CWE-621: Variable Extraction Error *(p.1385)*
- CWE-624: Executable Regular Expression Error *(p.1390)*
- CWE-627: Dynamic Variable Evaluation *(p.1396)*
- CWE-641: Improper Restriction of Names for Files and Other Resources *(p.1412)*
- CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') *(p.1419)*
- CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') *(p.1435)*
- CWE-692: Incomplete Denylist to Cross-Site Scripting *(p.1519)*
- CWE-694: Use of Multiple Resources with Duplicate Identifier *(p.1523)*
- CWE-914: Improper Control of Dynamically-Identified Variables *(p.1807)*
- CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') *(p.1818)*
- CWE-943: Improper Neutralization of Special Elements in Data Query Logic *(p.1850)*
- CWE-1236: Improper Neutralization of Formula Elements in a CSV File *(p.2019)*
- CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine *(p.2238)*

CWE-1410: Comprehensive Categorization: Insufficient Control Flow Management *(p.2536)*

- CWE-179: Incorrect Behavior Order: Early Validation *(p.448)*
- CWE-180: Incorrect Behavior Order: Validate Before Canonicalize *(p.451)*
- CWE-181: Incorrect Behavior Order: Validate Before Filter *(p.453)*
- CWE-248: Uncaught Exception *(p.596)*
- CWE-382: J2EE Bad Practices: Use of System.exit() *(p.933)*
- CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference *(p.957)*
- CWE-396: Declaration of Catch for Generic Exception *(p.959)*
- CWE-397: Declaration of Throws for Generic Exception *(p.961)*
- CWE-408: Incorrect Behavior Order: Early Amplification *(p.995)*
- CWE-430: Deployment of Wrong Handler *(p.1042)*
- CWE-431: Missing Handler *(p.1043)*
- CWE-455: Non-exit on Failed Initialization *(p.1087)*
- CWE-480: Use of Incorrect Operator *(p.1150)*
- CWE-481: Assigning instead of Comparing *(p.1154)*
- CWE-482: Comparing instead of Assigning *(p.1157)*
- CWE-483: Incorrect Block Delimitation *(p.1160)*
- CWE-584: Return Inside Finally Block *(p.1317)*
- CWE-600: Uncaught Exception in Servlet *(p.1343)*

- CWE-617: Reachable Assertion *(p.1378)*
- CWE-670: Always-Incorrect Control Flow Implementation *(p.1475)*
- CWE-674: Uncontrolled Recursion *(p.1484)*
- CWE-691: Insufficient Control Flow Management *(p.1517)*
- CWE-696: Incorrect Behavior Order *(p.1527)*
- CWE-698: Execution After Redirect (EAR) *(p.1533)*
- CWE-705: Incorrect Control Flow Scoping *(p.1542)*
- CWE-768: Incorrect Short Circuit Evaluation *(p.1612)*
- CWE-783: Operator Precedence Logic Error *(p.1650)*
- CWE-799: Improper Control of Interaction Frequency *(p.1699)*
- CWE-834: Excessive Iteration *(p.1754)*
- CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') *(p.1757)*
- CWE-837: Improper Enforcement of a Single, Unique Action *(p.1762)*
- CWE-841: Improper Enforcement of Behavioral Workflow *(p.1772)*
- CWE-1190: DMA Device Enabled Too Early in Boot Phase *(p.1978)*
- CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control *(p.1986)*
- CWE-1265: Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls *(p.2088)*
- CWE-1280: Access Control Check Implemented After Asset is Accessed *(p.2122)*
- CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior *(p.2124)*
- CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context *(p.2207)*

CWE-1411: Comprehensive Categorization: Insufficient Verification of Data Authenticity *(p.2538)*

- CWE-345: Insufficient Verification of Data Authenticity *(p.851)*
- CWE-346: Origin Validation Error *(p.853)*
- CWE-348: Use of Less Trusted Source *(p.859)*
- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data *(p.861)*
- CWE-351: Insufficient Type Distinction *(p.866)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-353: Missing Support for Integrity Check *(p.874)*
- CWE-354: Improper Validation of Integrity Check Value *(p.876)*
- CWE-360: Trust of System Event Data *(p.887)*
- CWE-494: Download of Code Without Integrity Check *(p.1185)*
- CWE-616: Incomplete Identification of Uploaded File Variables (PHP) *(p.1376)*
- CWE-646: Reliance on File Name or Extension of Externally-Supplied File *(p.1425)*
- CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking *(p.1430)*
- CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel *(p.1830)*
- CWE-1293: Missing Source Correlation of Multiple Independent Data *(p.2149)*
- CWE-1385: Missing Origin Validation in WebSockets *(p.2259)*

CWE-1399: Comprehensive Categorization: Memory Safety *(p.2525)*

- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') *(p.304)*
- CWE-121: Stack-based Buffer Overflow *(p.314)*
- CWE-122: Heap-based Buffer Overflow *(p.318)*
- CWE-123: Write-what-where Condition *(p.323)*
- CWE-124: Buffer Underwrite ('Buffer Underflow') *(p.326)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-126: Buffer Over-read *(p.334)*
- CWE-127: Buffer Under-read *(p.337)*
- CWE-129: Improper Validation of Array Index *(p.341)*
- CWE-131: Incorrect Calculation of Buffer Size *(p.355)*
- CWE-134: Use of Externally-Controlled Format String *(p.365)*
- CWE-188: Reliance on Data/Memory Layout *(p.470)*
- CWE-198: Use of Incorrect Byte Ordering *(p.503)*

- CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') *(p.591)*
- CWE-401: Missing Release of Memory after Effective Lifetime *(p.973)*
- CWE-415: Double Free *(p.1008)*
- CWE-416: Use After Free *(p.1012)*
- CWE-466: Return of Pointer Value Outside of Expected Range *(p.1109)*
- CWE-562: Return of Stack Variable Address *(p.1278)*
- CWE-587: Assignment of a Fixed Address to a Pointer *(p.1322)*
- CWE-590: Free of Memory not on the Heap *(p.1326)*
- CWE-680: Integer Overflow to Buffer Overflow *(p.1493)*
- CWE-690: Unchecked Return Value to NULL Pointer Dereference *(p.1514)*
- CWE-761: Free of Pointer not at Start of Buffer *(p.1592)*
- CWE-762: Mismatched Memory Management Routines *(p.1596)*
- CWE-763: Release of Invalid Pointer or Reference *(p.1599)*
- CWE-786: Access of Memory Location Before Start of Buffer *(p.1658)*
- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-788: Access of Memory Location After End of Buffer *(p.1669)*
- CWE-789: Memory Allocation with Excessive Size Value *(p.1674)*
- CWE-805: Buffer Access with Incorrect Length Value *(p.1702)*
- CWE-806: Buffer Access Using Size of Source Buffer *(p.1710)*
- CWE-822: Untrusted Pointer Dereference *(p.1723)*
- CWE-823: Use of Out-of-range Pointer Offset *(p.1726)*
- CWE-824: Access of Uninitialized Pointer *(p.1729)*
- CWE-825: Expired Pointer Dereference *(p.1732)*

CWE-1412: Comprehensive Categorization: Poor Coding Practices *(p.2538)*

- CWE-11: ASP.NET Misconfiguration: Creating Debug Binary *(p.9)*
- CWE-103: Struts: Incomplete validate() Method Definition *(p.248)*
- CWE-104: Struts: Form Bean Does Not Extend Validation Class *(p.251)*
- CWE-107: Struts: Unused Validation Form *(p.259)*
- CWE-110: Struts: Validator Without Form Field *(p.264)*
- CWE-111: Direct Use of Unsafe JNI *(p.266)*
- CWE-242: Use of Inherently Dangerous Function *(p.586)*
- CWE-245: J2EE Bad Practices: Direct Management of Connections *(p.592)*
- CWE-246: J2EE Bad Practices: Direct Use of Sockets *(p.594)*
- CWE-253: Incorrect Check of Function Return Value *(p.613)*
- CWE-358: Improperly Implemented Security Check for Standard *(p.881)*
- CWE-383: J2EE Bad Practices: Direct Use of Threads *(p.935)*
- CWE-392: Missing Report of Error Condition *(p.951)*
- CWE-393: Return of Wrong Status Code *(p.953)*
- CWE-440: Expected Behavior Violation *(p.1062)*
- CWE-446: UI Discrepancy for Security Feature *(p.1073)*
- CWE-448: Obsolete Feature in UI *(p.1076)*
- CWE-449: The UI Performs the Wrong Action *(p.1077)*
- CWE-451: User Interface (UI) Misrepresentation of Critical Information *(p.1079)*
- CWE-462: Duplicate Key in Associative List (Alist) *(p.1104)*
- CWE-474: Use of Function with Inconsistent Implementations *(p.1128)*
- CWE-475: Undefined Behavior for Input to API *(p.1130)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-477: Use of Obsolete Function *(p.1138)*
- CWE-484: Omitted Break Statement in Switch *(p.1162)*
- CWE-489: Active Debug Code *(p.1171)*
- CWE-506: Embedded Malicious Code *(p.1210)*
- CWE-507: Trojan Horse *(p.1212)*
- CWE-508: Non-Replicating Malicious Code *(p.1213)*
- CWE-509: Replicating Malicious Code (Virus or Worm) *(p.1214)*

- CWE-510: Trapdoor *(p.1215)*
- CWE-511: Logic/Time Bomb *(p.1216)*
- CWE-512: Spyware *(p.1218)*
- CWE-546: Suspicious Comment *(p.1258)*
- CWE-547: Use of Hard-coded, Security-relevant Constants *(p.1259)*
- CWE-560: Use of umask() with chmod-style Argument *(p.1274)*
- CWE-561: Dead Code *(p.1275)*
- CWE-563: Assignment to Variable without Use *(p.1280)*
- CWE-570: Expression is Always False *(p.1292)*
- CWE-571: Expression is Always True *(p.1295)*
- CWE-573: Improper Following of Specification by Caller *(p.1298)*
- CWE-575: EJB Bad Practices: Use of AWT Swing *(p.1301)*
- CWE-576: EJB Bad Practices: Use of Java I/O *(p.1304)*
- CWE-577: EJB Bad Practices: Use of Sockets *(p.1305)*
- CWE-578: EJB Bad Practices: Use of Class Loader *(p.1307)*
- CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session *(p.1309)*
- CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined *(p.1312)*
- CWE-585: Empty Synchronized Block *(p.1318)*
- CWE-586: Explicit Call to Finalize() *(p.1320)*
- CWE-589: Call to Non-ubiquitous API *(p.1325)*
- CWE-594: J2EE Framework: Saving Unserializable Objects to Disk *(p.1332)*
- CWE-605: Multiple Binds to the Same Port *(p.1356)*
- CWE-628: Function Call with Incorrectly Specified Arguments *(p.1398)*
- CWE-675: Multiple Operations on Resource in Single-Operation Context *(p.1487)*
- CWE-676: Use of Potentially Dangerous Function *(p.1489)*
- CWE-683: Function Call With Incorrect Order of Arguments *(p.1504)*
- CWE-684: Incorrect Provision of Specified Functionality *(p.1505)*
- CWE-685: Function Call With Incorrect Number of Arguments *(p.1507)*
- CWE-686: Function Call With Incorrect Argument Type *(p.1508)*
- CWE-687: Function Call With Incorrectly Specified Argument Value *(p.1510)*
- CWE-688: Function Call With Incorrect Variable or Reference as Argument *(p.1511)*
- CWE-695: Use of Low-Level Functionality *(p.1524)*
- CWE-710: Improper Adherence to Coding Standards *(p.1549)*
- CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior *(p.1582)*
- CWE-766: Critical Data Element Declared Public *(p.1607)*
- CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer *(p.1656)*
- CWE-912: Hidden Functionality *(p.1803)*
- CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User *(p.1857)*
- CWE-1041: Use of Redundant Code *(p.1875)*
- CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements *(p.1877)*
- CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range *(p.1879)*
- CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor *(p.1880)*
- CWE-1047: Modules with Circular Dependencies *(p.1882)*
- CWE-1048: Invokable Control Element with Large Number of Outward Calls *(p.1883)*
- CWE-1053: Missing Documentation for Design *(p.1888)*
- CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer *(p.1889)*
- CWE-1055: Multiple Inheritance from Concrete Classes *(p.1890)*
- CWE-1056: Invokable Control Element with Variadic Parameters *(p.1891)*
- CWE-1057: Data Access Operations Outside of Expected Data Manager Component *(p.1892)*
- CWE-1059: Insufficient Technical Documentation *(p.1894)*
- CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses *(p.1897)*
- CWE-1061: Insufficient Encapsulation *(p.1898)*

- CWE-1062: Parent Class with References to Child Class *(p.1900)*
- CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters *(p.1902)*
- CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers *(p.1903)*
- CWE-1066: Missing Serialization Control Element *(p.1904)*
- CWE-1068: Inconsistency Between Implementation and Documented Design *(p.1906)*
- CWE-1069: Empty Exception Block *(p.1907)*
- CWE-1070: Serializable Data Element Containing non-Serializable Item Elements *(p.1909)*
- CWE-1071: Empty Code Block *(p.1910)*
- CWE-1074: Class with Excessively Deep Inheritance *(p.1914)*
- CWE-1075: Unconditional Control Flow Transfer outside of Switch Block *(p.1915)*
- CWE-1076: Insufficient Adherence to Expected Conventions *(p.1916)*
- CWE-1078: Inappropriate Source Code Style or Formatting *(p.1918)*
- CWE-1079: Parent Class without Virtual Destructor Method *(p.1919)*
- CWE-1080: Source Code File with Excessive Number of Lines of Code *(p.1920)*
- CWE-1082: Class Instance Self Destruction Control Element *(p.1921)*
- CWE-1083: Data Access from Outside Expected Data Manager Component *(p.1922)*
- CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code *(p.1925)*
- CWE-1086: Class with Excessive Number of Child Classes *(p.1926)*
- CWE-1087: Class with Virtual Method without a Virtual Destructor *(p.1927)*
- CWE-1090: Method Containing Access of a Member Element from Another Class *(p.1930)*
- CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers *(p.1932)*
- CWE-1093: Excessively Complex Data Representation *(p.1933)*
- CWE-1095: Loop Condition Value Update within the Loop *(p.1935)*
- CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element *(p.1937)*
- CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element *(p.1938)*
- CWE-1099: Inconsistent Naming Conventions for Identifiers *(p.1939)*
- CWE-1100: Insufficient Isolation of System-Dependent Functions *(p.1940)*
- CWE-1101: Reliance on Runtime Component in Generated Code *(p.1941)*
- CWE-1102: Reliance on Machine-Dependent Data Representation *(p.1942)*
- CWE-1103: Use of Platform-Dependent Third Party Components *(p.1943)*
- CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality *(p.1945)*
- CWE-1106: Insufficient Use of Symbolic Constants *(p.1946)*
- CWE-1107: Insufficient Isolation of Symbolic Constant Definitions *(p.1947)*
- CWE-1108: Excessive Reliance on Global Variables *(p.1948)*
- CWE-1109: Use of Same Variable for Multiple Purposes *(p.1949)*
- CWE-1110: Incomplete Design Documentation *(p.1950)*
- CWE-1111: Incomplete I/O Documentation *(p.1951)*
- CWE-1112: Incomplete Documentation of Program Execution *(p.1952)*
- CWE-1113: Inappropriate Comment Style *(p.1953)*
- CWE-1114: Inappropriate Whitespace Style *(p.1953)*
- CWE-1115: Source Code Element without Standard Prologue *(p.1954)*
- CWE-1116: Inaccurate Comments *(p.1955)*
- CWE-1117: Callable with Insufficient Behavioral Summary *(p.1957)*
- CWE-1118: Insufficient Documentation of Error Handling Techniques *(p.1958)*
- CWE-1119: Excessive Use of Unconditional Branching *(p.1959)*
- CWE-1120: Excessive Code Complexity *(p.1960)*
- CWE-1121: Excessive McCabe Cyclomatic Complexity *(p.1961)*
- CWE-1122: Excessive Halstead Complexity *(p.1962)*
- CWE-1123: Excessive Use of Self-Modifying Code *(p.1963)*
- CWE-1124: Excessively Deep Nesting *(p.1964)*
- CWE-1125: Excessive Attack Surface *(p.1965)*

- CWE-1126: Declaration of Variable with Unnecessarily Wide Scope *(p.1966)*
- CWE-1127: Compilation with Insufficient Warnings or Errors *(p.1966)*
- CWE-1164: Irrelevant Code *(p.1967)*
- CWE-1177: Use of Prohibited Code *(p.1972)*
- CWE-1209: Failure to Disable Reserved Bits *(p.1991)*
- CWE-1245: Improper Finite State Machines (FSMs) in Hardware Logic *(p.2041)*
- CWE-1341: Multiple Releases of Same Resource or Handle *(p.2246)*
- CWE-1357: Reliance on Insufficiently Trustworthy Component *(p.2254)*

CWE-1413: Comprehensive Categorization: Protection Mechanism Failure *(p.2542)*

- CWE-182: Collapse of Data into Unsafe Value *(p.455)*
- CWE-184: Incomplete List of Disallowed Inputs *(p.459)*
- CWE-222: Truncation of Security-relevant Information *(p.557)*
- CWE-223: Omission of Security-relevant Information *(p.559)*
- CWE-224: Obscured Security-relevant Information by Alternate Name *(p.561)*
- CWE-356: Product UI does not Warn User of Unsafe Actions *(p.879)*
- CWE-357: Insufficient UI Warning of Dangerous Operations *(p.880)*
- CWE-450: Multiple Interpretations of UI Input *(p.1078)*
- CWE-602: Client-Side Enforcement of Server-Side Security *(p.1350)*
- CWE-693: Protection Mechanism Failure *(p.1520)*
- CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') *(p.1581)*
- CWE-778: Insufficient Logging *(p.1638)*
- CWE-807: Reliance on Untrusted Inputs in a Security Decision *(p.1714)*
- CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations *(p.1873)*
- CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications *(p.2049)*
- CWE-1253: Incorrect Selection of Fuse Values *(p.2058)*
- CWE-1269: Product Released in Non-Release Configuration *(p.2098)*
- CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques *(p.2118)*
- CWE-1291: Public Key Re-Use for Signing both Debug and Production Code *(p.2145)*
- CWE-1318: Missing Support for Security Features in On-chip Fabrics or Buses *(p.2197)*
- CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) *(p.2199)*
- CWE-1326: Missing Immutable Root of Trust in Hardware *(p.2212)*
- CWE-1338: Improper Protections Against Hardware Overheating *(p.2240)*

CWE-1414: Comprehensive Categorization: Randomness *(p.2543)*

- CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length *(p.2)*
- CWE-323: Reusing a Nonce, Key Pair in Encryption *(p.790)*
- CWE-329: Generation of Predictable IV with CBC Mode *(p.811)*
- CWE-330: Use of Insufficiently Random Values *(p.814)*
- CWE-331: Insufficient Entropy *(p.821)*
- CWE-332: Insufficient Entropy in PRNG *(p.823)*
- CWE-333: Improper Handling of Insufficient Entropy in TRNG *(p.825)*
- CWE-334: Small Space of Random Values *(p.827)*
- CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) *(p.829)*
- CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) *(p.832)*
- CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) *(p.834)*
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) *(p.837)*
- CWE-339: Small Seed Space in PRNG *(p.840)*
- CWE-340: Generation of Predictable Numbers or Identifiers *(p.842)*
- CWE-341: Predictable from Observable State *(p.843)*
- CWE-342: Predictable Exact Value from Previous Values *(p.845)*
- CWE-343: Predictable Value Range from Previous Values *(p.847)*
- CWE-344: Use of Invariant Value in Dynamically Changing Context *(p.849)*
- CWE-1204: Generation of Weak Initialization Vector (IV) *(p.1987)*

- CWE-1241: Use of Predictable Algorithm in Random Number Generator *(p.2030)*

CWE-1415: Comprehensive Categorization: Resource Control *(p.2544)*
- CWE-385: Covert Timing Channel *(p.940)*
- CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') *(p.1118)*
- CWE-473: PHP External Variable Modification *(p.1127)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-514: Covert Channel *(p.1218)*
- CWE-515: Covert Storage Channel *(p.1220)*
- CWE-672: Operation on a Resource after Expiration or Release *(p.1479)*
- CWE-826: Premature Release of Resource During Expected Lifetime *(p.1734)*
- CWE-910: Use of Expired File Descriptor *(p.1800)*
- CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes *(p.1809)*
- CWE-1104: Use of Unmaintained Third Party Components *(p.1944)*
- CWE-1249: Application-Level Admin Tool with Inconsistent View of Underlying Operating System *(p.2050)*
- CWE-1251: Mirrored Regions with Different Values *(p.2054)*
- CWE-1277: Firmware Not Updateable *(p.2116)*
- CWE-1310: Missing Ability to Patch ROM Code *(p.2179)*
- CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') *(p.2204)*
- CWE-1329: Reliance on Component That is Not Updateable *(p.2219)*

CWE-1416: Comprehensive Categorization: Resource Lifecycle Management *(p.2545)*
- CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') *(p.236)*
- CWE-118: Incorrect Access of Indexable Resource ('Range Error') *(p.292)*
- CWE-178: Improper Handling of Case Sensitivity *(p.445)*
- CWE-192: Integer Coercion Error *(p.482)*
- CWE-194: Unexpected Sign Extension *(p.491)*
- CWE-195: Signed to Unsigned Conversion Error *(p.494)*
- CWE-196: Unsigned to Signed Conversion Error *(p.498)*
- CWE-197: Numeric Truncation Error *(p.500)*
- CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer *(p.544)*
- CWE-221: Information Loss or Omission *(p.556)*
- CWE-226: Sensitive Information in Resource Not Removed Before Reuse *(p.562)*
- CWE-243: Creation of chroot Jail Without Changing Working Directory *(p.589)*
- CWE-372: Incomplete Internal State Distinction *(p.919)*
- CWE-386: Symbolic Name not Mapping to Correct Object *(p.942)*
- CWE-400: Uncontrolled Resource Consumption *(p.964)*
- CWE-404: Improper Resource Shutdown or Release *(p.980)*
- CWE-405: Asymmetric Resource Consumption (Amplification) *(p.986)*
- CWE-406: Insufficient Control of Network Message Volume (Network Amplification) *(p.990)*
- CWE-407: Inefficient Algorithmic Complexity *(p.992)*
- CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) *(p.996)*
- CWE-410: Insufficient Resource Pool *(p.998)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-453: Insecure Default Variable Initialization *(p.1083)*
- CWE-454: External Initialization of Trusted Variables or Data Stores *(p.1085)*
- CWE-456: Missing Initialization of a Variable *(p.1089)*
- CWE-457: Use of Uninitialized Variable *(p.1094)*
- CWE-459: Incomplete Cleanup *(p.1099)*
- CWE-460: Improper Cleanup on Thrown Exception *(p.1102)*
- CWE-471: Modification of Assumed-Immutable Data (MAID) *(p.1121)*
- CWE-487: Reliance on Package-level Scope *(p.1167)*
- CWE-495: Private Data Structure Returned From A Public Method *(p.1189)*

- CWE-496: Public Data Assigned to Private Array-Typed Field *(p.1192)*
- CWE-501: Trust Boundary Violation *(p.1203)*
- CWE-568: finalize() Method Without super.finalize() *(p.1290)*
- CWE-580: clone() Method Without super.clone() *(p.1311)*
- CWE-588: Attempt to Access Child of a Non-structure Pointer *(p.1323)*
- CWE-607: Public Static Final Field References Mutable Object *(p.1360)*
- CWE-610: Externally Controlled Reference to a Resource in Another Sphere *(p.1364)*
- CWE-618: Exposed Unsafe ActiveX Method *(p.1380)*
- CWE-662: Improper Synchronization *(p.1448)*
- CWE-664: Improper Control of a Resource Through its Lifetime *(p.1454)*
- CWE-665: Improper Initialization *(p.1456)*
- CWE-666: Operation on Resource in Wrong Phase of Lifetime *(p.1462)*
- CWE-669: Incorrect Resource Transfer Between Spheres *(p.1471)*
- CWE-673: External Influence of Sphere Definition *(p.1483)*
- CWE-681: Incorrect Conversion between Numeric Types *(p.1495)*
- CWE-704: Incorrect Type Conversion or Cast *(p.1538)*
- CWE-706: Use of Incorrectly-Resolved Name or Reference *(p.1544)*
- CWE-749: Exposed Dangerous Method or Function *(p.1564)*
- CWE-770: Allocation of Resources Without Limits or Throttling *(p.1613)*
- CWE-771: Missing Reference to Active Allocated Resource *(p.1622)*
- CWE-772: Missing Release of Resource after Effective Lifetime *(p.1624)*
- CWE-773: Missing Reference to Active File Descriptor or Handle *(p.1629)*
- CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling *(p.1630)*
- CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime *(p.1631)*
- CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') *(p.1633)*
- CWE-779: Logging of Excessive Data *(p.1642)*
- CWE-782: Exposed IOCTL with Insufficient Access Control *(p.1648)*
- CWE-827: Improper Control of Document Type Definition *(p.1736)*
- CWE-829: Inclusion of Functionality from Untrusted Control Sphere *(p.1741)*
- CWE-830: Inclusion of Web Functionality from an Untrusted Source *(p.1747)*
- CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') *(p.1776)*
- CWE-908: Use of Uninitialized Resource *(p.1792)*
- CWE-909: Missing Initialization of Resource *(p.1797)*
- CWE-911: Improper Update of Reference Count *(p.1801)*
- CWE-913: Improper Control of Dynamically-Managed Code Resources *(p.1805)*
- CWE-920: Improper Restriction of Power Consumption *(p.1823)*
- CWE-922: Insecure Storage of Sensitive Information *(p.1825)*
- CWE-1042: Static Member Data Element outside of a Singleton Class Element *(p.1876)*
- CWE-1046: Creation of Immutable Text Using String Concatenation *(p.1881)*
- CWE-1049: Excessive Data Query Operations in a Large Data Table *(p.1884)*
- CWE-1050: Excessive Platform Resource Consumption within a Loop *(p.1885)*
- CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data *(p.1886)*
- CWE-1052: Excessive Use of Hard-Coded Literals in Initialization *(p.1887)*
- CWE-1063: Creation of Class Instance within a Static Code Block *(p.1901)*
- CWE-1067: Excessive Execution of Sequential Searches of Data Resource *(p.1905)*
- CWE-1072: Data Resource Access without Use of Connection Pooling *(p.1912)*
- CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses *(p.1913)*
- CWE-1084: Invokable Control Element with Excessive File or Data Access Operations *(p.1924)*
- CWE-1089: Large Data Table with Excessive Number of Indices *(p.1929)*
- CWE-1091: Use of Object without Invoking Destructor Method *(p.1931)*
- CWE-1094: Excessive Index Range Scan for a Data Resource *(p.1934)*
- CWE-1176: Inefficient CPU Computation *(p.1971)*

- CWE-1188: Initialization of a Resource with an Insecure Default *(p.1974)*
- CWE-1221: Incorrect Register Defaults or Module Parameters *(p.1996)*
- CWE-1229: Creation of Emergent Resource *(p.2006)*
- CWE-1235: Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations *(p.2017)*
- CWE-1239: Improper Zeroization of Hardware Register *(p.2022)*
- CWE-1246: Improper Write Handling in Limited-write Non-Volatile Memories *(p.2043)*
- CWE-1250: Improper Preservation of Consistency Between Independent Representations of Shared State *(p.2052)*
- CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information *(p.2071)*
- CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device *(p.2091)*
- CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings *(p.2102)*
- CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition *(p.2104)*
- CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready *(p.2120)*
- CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component *(p.2170)*
- CWE-1325: Improperly Controlled Sequential Memory Allocation *(p.2210)*
- CWE-1330: Remanent Data Readable after Memory Erase *(p.2222)*
- CWE-1333: Inefficient Regular Expression Complexity *(p.2230)*
- CWE-1342: Information Exposure through Microarchitectural State after Transient Execution *(p.2250)*
- CWE-1386: Insecure Operation on Windows Junction / Mount Point *(p.2261)*
- CWE-1389: Incorrect Parsing of Numbers with Different Radices *(p.2263)*
- CWE-1419: Incorrect Initialization of Resource *(p.2280)*
- CWE-1420: Exposure of Sensitive Information during Transient Execution *(p.2284)*
- CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution *(p.2290)*
- CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution *(p.2297)*
- CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution *(p.2302)*

CWE-1417: Comprehensive Categorization: Sensitive Information Exposure *(p.2548)*

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor *(p.504)*
- CWE-201: Insertion of Sensitive Information Into Sent Data *(p.514)*
- CWE-203: Observable Discrepancy *(p.518)*
- CWE-204: Observable Response Discrepancy *(p.523)*
- CWE-205: Observable Behavioral Discrepancy *(p.526)*
- CWE-206: Observable Internal Behavioral Discrepancy *(p.527)*
- CWE-207: Observable Behavioral Discrepancy With Equivalent Products *(p.528)*
- CWE-208: Observable Timing Discrepancy *(p.529)*
- CWE-209: Generation of Error Message Containing Sensitive Information *(p.533)*
- CWE-210: Self-generated Error Message Containing Sensitive Information *(p.539)*
- CWE-211: Externally-Generated Error Message Containing Sensitive Information *(p.541)*
- CWE-213: Exposure of Sensitive Information Due to Incompatible Policies *(p.547)*
- CWE-214: Invocation of Process Using Visible Sensitive Information *(p.549)*
- CWE-215: Insertion of Sensitive Information Into Debugging Code *(p.551)*
- CWE-359: Exposure of Private Personal Information to an Unauthorized Actor *(p.882)*
- CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere *(p.1193)*
- CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable *(p.1234)*
- CWE-531: Inclusion of Sensitive Information in Test Code *(p.1240)*
- CWE-532: Insertion of Sensitive Information into Log File *(p.1241)*
- CWE-535: Exposure of Information Through Shell Error Message *(p.1244)*
- CWE-536: Servlet Runtime Error Message Containing Sensitive Information *(p.1245)*
- CWE-537: Java Runtime Error Message Containing Sensitive Information *(p.1246)*
- CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory *(p.1248)*
- CWE-540: Inclusion of Sensitive Information in Source Code *(p.1251)*
- CWE-541: Inclusion of Sensitive Information in an Include File *(p.1253)*
- CWE-548: Exposure of Information Through Directory Listing *(p.1261)*

- CWE-550: Server-generated Error Message Containing Sensitive Information *(p.1263)*
- CWE-598: Use of GET Request Method With Sensitive Query Strings *(p.1340)*
- CWE-615: Inclusion of Sensitive Information in Source Code Comments *(p.1375)*
- CWE-651: Exposure of WSDL File Containing Sensitive Information *(p.1433)*
- CWE-1254: Incorrect Comparison Logic Granularity *(p.2060)*
- CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks *(p.2062)*
- CWE-1273: Device Unlock Credential Sharing *(p.2106)*
- CWE-1295: Debug Messages Revealing Unnecessary Information *(p.2152)*
- CWE-1300: Improper Protection of Physical Side Channels *(p.2165)*

CWE-1418: Comprehensive Categorization: Violation of Secure Design Principles *(p.2549)*

- CWE-250: Execution with Unnecessary Privileges *(p.599)*
- CWE-424: Improper Protection of Alternate Path *(p.1023)*
- CWE-447: Unimplemented or Unsupported Feature in UI *(p.1075)*
- CWE-636: Not Failing Securely ('Failing Open') *(p.1401)*
- CWE-637: Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism') *(p.1403)*
- CWE-638: Not Using Complete Mediation *(p.1404)*
- CWE-653: Improper Isolation or Compartmentalization *(p.1437)*
- CWE-654: Reliance on a Single Factor in a Security Decision *(p.1439)*
- CWE-655: Insufficient Psychological Acceptability *(p.1442)*
- CWE-656: Reliance on Security Through Obscurity *(p.1444)*
- CWE-657: Violation of Secure Design Principles *(p.1446)*
- CWE-671: Lack of Administrator Control over Security *(p.1478)*
- CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) *(p.1976)*
- CWE-1192: Improper Identifier for IP Block used in System-On-Chip (SOC) *(p.1985)*
- CWE-1303: Non-Transparent Sharing of Microarchitectural Resources *(p.2174)*
- CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) *(p.2225)*
- CWE-1395: Dependency on Vulnerable Third-Party Component *(p.2277)*

Graph View: CWE-1425: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses

- CWE-787: Out-of-bounds Write *(p.1661)*
- CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') *(p.163)*
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') *(p.201)*
- CWE-416: Use After Free *(p.1012)*
- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') *(p.151)*
- CWE-20: Improper Input Validation *(p.20)*
- CWE-125: Out-of-bounds Read *(p.330)*
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') *(p.33)*
- CWE-352: Cross-Site Request Forgery (CSRF) *(p.868)*
- CWE-434: Unrestricted Upload of File with Dangerous Type *(p.1048)*
- CWE-862: Missing Authorization *(p.1780)*
- CWE-476: NULL Pointer Dereference *(p.1132)*
- CWE-287: Improper Authentication *(p.692)*
- CWE-190: Integer Overflow or Wraparound *(p.472)*
- CWE-502: Deserialization of Untrusted Data *(p.1204)*
- CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') *(p.145)*
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer *(p.293)*
- CWE-798: Use of Hard-coded Credentials *(p.1690)*
- CWE-918: Server-Side Request Forgery (SSRF) *(p.1820)*
- CWE-306: Missing Authentication for Critical Function *(p.741)*
- CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') *(p.888)*
- CWE-269: Improper Privilege Management *(p.646)*
- CWE-94: Improper Control of Generation of Code ('Code Injection') *(p.219)*
- CWE-863: Incorrect Authorization *(p.1787)*
- CWE-276: Incorrect Default Permissions *(p.665)*

Deprecated

CWE-1: DEPRECATED: Location

CWE ID : 1

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-3: DEPRECATED: Technology-specific Environment Issues

CWE ID : 3

Summary

This category has been deprecated. It was originally intended as a "catch-all" for environment issues for technologies that did not have their own CWE, but it introduced unnecessary depth and complexity to the Development View (CWE-699).

CWE-4: DEPRECATED: J2EE Environment Issues

CWE ID : 4

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-10: DEPRECATED: ASP.NET Environment Issues

CWE ID : 10

Summary

This category has been deprecated. It added unnecessary depth and complexity to its associated views.

CWE-17: DEPRECATED: Code

CWE ID : 17

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-18: DEPRECATED: Source Code

CWE ID : 18

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-21: DEPRECATED: Pathname Traversal and Equivalence Errors

CWE ID : 21

Summary

This category has been deprecated. It was originally used for organizing weaknesses involving file names, which enabled access to files outside of a restricted directory (path traversal) or to perform operations on files that would otherwise be restricted (path equivalence). Consider using either the File Handling Issues category (CWE-1219) or the class Use of Incorrectly-Resolved Name or Reference (CWE-706).

CWE-60: DEPRECATED: UNIX Path Link Problems

CWE ID : 60

Summary

This category has been deprecated. It covered a very low level of abstraction based on operating system, which was not useful for any existing view.

CWE-63: DEPRECATED: Windows Path Link Problems

CWE ID : 63

Summary

This category has been deprecated. It covered a very low level of abstraction based on operating system, which was not useful for any existing view.

CWE-68: DEPRECATED: Windows Virtual File Problems

CWE ID : 68

Summary

This category has been deprecated as it was found to be an unnecessary abstraction of platform specific details. Please refer to the category CWE-632 and weakness CWE-66 for relevant relationships.

CWE-70: DEPRECATED: Mac Virtual File Problems

CWE ID : 70

Summary

This category has been deprecated as it was found to be an unnecessary abstraction of platform specific details. Please refer to the category CWE-632 and weakness CWE-66 for relevant relationships.

CWE-71: DEPRECATED: Apple '.DS_Store'

CWE ID : 71

Description

This entry has been deprecated as it represents a specific observed example of a UNIX Hard Link weakness type rather than its own individual weakness type. Please refer to CWE-62.

CWE-92: DEPRECATED: Improper Sanitization of Custom Special Characters

CWE ID : 92

Description

This entry has been deprecated. It originally came from PLOVER, which sometimes defined "other" and "miscellaneous" categories in order to satisfy exhaustiveness requirements for taxonomies. Within the context of CWE, the use of a more abstract entry is preferred in mapping situations. CWE-75 is a more appropriate mapping.

CWE-100: DEPRECATED: Technology-Specific Input Validation Problems

CWE ID : 100

Summary

This category has been deprecated. It was originally intended as a "catch-all" for input validation problems in technologies that did not have their own CWE, but introduces unnecessary depth to the hierarchy.

CWE-101: DEPRECATED: Struts Validation Problems

CWE ID : 101

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-132: DEPRECATED: Miscalculated Null Termination

CWE ID : 132

Description

This entry has been deprecated because it was a duplicate of CWE-170. All content has been transferred to CWE-170.

CWE-139: DEPRECATED: General Special Element Problems

CWE ID : 139

Summary

This entry has been deprecated. It is a leftover from PLOVER, but CWE-138 is a more appropriate mapping.

CWE-169: DEPRECATED: Technology-Specific Special Elements

CWE ID : 169

Summary

This category has been deprecated. It was originally intended as a "catch-all" for input validation problems in technologies that did not have their own CWE, but introduces unnecessary depth to the hierarchy.

CWE-171: DEPRECATED: Cleansing, Canonicalization, and Comparison Errors

CWE ID : 171

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree. Weaknesses in this category were related to improper handling of data within protection mechanisms that attempt to perform neutralization for untrusted data. These weaknesses can be found in other similar categories.

CWE-216: DEPRECATED: Containment Errors (Container Errors)

CWE ID : 216

Description

This entry has been deprecated, as it was not effective as a weakness and was structured more like a category. In addition, the name is inappropriate, since the "container" term is widely understood by developers in different ways than originally intended by PLOVER, the original source for this entry.

CWE-217: DEPRECATED: Failure to Protect Stored Data from Modification

CWE ID : 217

Description

This entry has been deprecated because it incorporated and confused multiple weaknesses. The issues formerly covered in this entry can be found at CWE-766 and CWE-767.

CWE-218: DEPRECATED: Failure to provide confidentiality for stored data

CWE ID : 218

Description

This weakness has been deprecated because it was a duplicate of CWE-493. All content has been transferred to CWE-493.

CWE-225: DEPRECATED: General Information Management Problems

CWE ID : 225

Description

This weakness can be found at CWE-199.

CWE-247: DEPRECATED: Reliance on DNS Lookups in a Security Decision

CWE ID : 247

Description

This entry has been deprecated because it was a duplicate of CWE-350. All content has been transferred to CWE-350.

CWE-249: DEPRECATED: Often Misused: Path Manipulation

CWE ID : 249

Description

This entry has been deprecated because of name confusion and an accidental combination of multiple weaknesses. Most of its content has been transferred to CWE-785.

CWE-292: DEPRECATED: Trusting Self-reported DNS Name

CWE ID : 292

Description

This entry has been deprecated because it was a duplicate of CWE-350. All content has been transferred to CWE-350.

CWE-365: DEPRECATED: Race Condition in Switch

CWE ID : 365

Description

This entry has been deprecated. There are no documented cases in which a switch's control expression is evaluated more than once.

CWE-373: DEPRECATED: State Synchronization Error

CWE ID : 373

Description

This entry was deprecated because it overlapped the same concepts as race condition (CWE-362) and Improper Synchronization (CWE-662).

CWE-376: DEPRECATED: Temporary File Issues

CWE ID : 376

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree. Consider using the File Handling Issues category (CWE-1219).

CWE-380: DEPRECATED: Technology-Specific Time and State Issues

CWE ID : 380

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-381: DEPRECATED: J2EE Time and State Issues

CWE ID : 381

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-418: DEPRECATED: Channel Errors

CWE ID : 418

Summary

This category has been deprecated because it redundant with the grouping provided by CWE-417.

CWE-423: DEPRECATED: Proxied Trusted Channel

CWE ID : 423

Description

This entry has been deprecated because it was a duplicate of CWE-441. All content has been transferred to CWE-441.

CWE-442: DEPRECATED: Web Problems

CWE ID : 442

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-443: DEPRECATED: HTTP response splitting

CWE ID : 443

Description

This weakness can be found at CWE-113.

CWE-445: DEPRECATED: User Interface Errors

CWE ID : 445

Summary

This weakness has been deprecated because it was a duplicate of CWE-355. All content has been transferred to CWE-355.

CWE-458: DEPRECATED: Incorrect Initialization

CWE ID : 458

Description

This weakness has been deprecated because its name and description did not match. The description duplicated CWE-454, while the name suggested a more abstract initialization problem. Please refer to CWE-665 for the more abstract problem.

CWE-461: DEPRECATED: Data Structure Issues

CWE ID : 461

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-490: DEPRECATED: Mobile Code Issues

CWE ID : 490

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-503: DEPRECATED: Byte/Object Code

CWE ID : 503

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-504: DEPRECATED: Motivation/Intent

CWE ID : 504

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-505: DEPRECATED: Intentionally Introduced Weakness

CWE ID : 505

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-513: DEPRECATED: Intentionally Introduced Nonmalicious Weakness

CWE ID : 513

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-516: DEPRECATED: Covert Timing Channel

CWE ID : 516

Description

This weakness can be found at CWE-385.

CWE-517: DEPRECATED: Other Intentional, Nonmalicious Weakness

CWE ID : 517

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-518: DEPRECATED: Inadvertently Introduced Weakness

CWE ID : 518

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-519: DEPRECATED: .NET Environment Issues

CWE ID : 519

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-533: DEPRECATED: Information Exposure Through Server Log Files

CWE ID : 533

Description

This entry has been deprecated because its abstraction was too low-level. See CWE-532.

CWE-534: DEPRECATED: Information Exposure Through Debug Log Files

CWE ID : 534

Description

This entry has been deprecated because its abstraction was too low-level. See CWE-532.

CWE-542: DEPRECATED: Information Exposure Through Cleanup Log Files

CWE ID : 542

Description

This entry has been deprecated because its abstraction was too low-level. See CWE-532.

CWE-545: DEPRECATED: Use of Dynamic Class Loading

CWE ID : 545

Description

This weakness has been deprecated because it partially overlaps CWE-470, it describes legitimate programmer behavior, and other portions will need to be integrated into other entries.

CWE-559: DEPRECATED: Often Misused: Arguments and Parameters

CWE ID : 559

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-592: DEPRECATED: Authentication Bypass Issues

CWE ID : 592

Description

This weakness has been deprecated because it covered redundant concepts already described in CWE-287.

CWE-596: DEPRECATED: Incorrect Semantic Object Comparison

CWE ID : 596

Description

This weakness has been deprecated. It was poorly described and difficult to distinguish from other entries. It was also inappropriate to assign a separate ID solely because of domain-specific considerations. Its closest equivalent is CWE-1023.

CWE-630: DEPRECATED: Weaknesses Examined by SAMATE

CWE ID : 630

Objective

This view has been deprecated. It was only used for an early year of the NIST SAMATE project, and it did not represent any official or commonly-utilized list.

CWE-631: DEPRECATED: Resource-specific Weaknesses

CWE ID : 631

Objective

This view has been deprecated because it is not actively maintained and does not provide utility to stakeholders. It was originally created before CWE 1.0 as a simple example of how views could be structured within CWE.

CWE-632: DEPRECATED: Weaknesses that Affect Files or Directories

CWE ID : 632

Summary

This category has been deprecated. It was not actively maintained, and it was not useful to stakeholders. It was originally created before CWE 1.0 as part of view CWE-631, which was a simple example of how views could be structured within CWE.

CWE-633: DEPRECATED: Weaknesses that Affect Memory

CWE ID : 633

Summary

This category has been deprecated. It was not actively maintained, and it was not useful to stakeholders. It was originally created before CWE 1.0 as part of view CWE-631, which was a simple example of how views could be structured within CWE.

CWE-634: DEPRECATED: Weaknesses that Affect System Processes

CWE ID : 634

Summary

This category has been deprecated. It was not actively maintained, and it was not useful to stakeholders. It was originally created before CWE 1.0 as part of view CWE-631, which was a simple example of how views could be structured within CWE.

CWE-679: DEPRECATED: Chain Elements

CWE ID : 679

Objective

This view has been deprecated. It has limited utility for stakeholders, since all weaknesses can be links in a chain.

CWE-769: DEPRECATED: Uncontrolled File Descriptor Consumption

CWE ID : 769

Description

This entry has been deprecated because it was a duplicate of CWE-774. All content has been transferred to CWE-774.

CWE-999: DEPRECATED: Weaknesses without Software Fault Patterns

CWE ID : 999

Objective

This view has been deprecated. It was based on gaps in another view (CWE-888) related to research that is no longer updated, but was complete with respect to CWE at the time it was conducted.

CWE-1187: DEPRECATED: Use of Uninitialized Resource

CWE ID : 1187

Description

This entry has been deprecated because it was a duplicate of CWE-908. All content has been transferred to CWE-908.

CWE-1324: DEPRECATED: Sensitive Information Accessible by Physical Probing of JTAG Interface

CWE ID : 1324

Description

This entry has been deprecated because it was at a lower level of abstraction than supported by CWE. All relevant content has been integrated into CWE-319.

Glossary

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X