Auflistung der in „Chess Online“ auffindbaren CWEs

Nachfolgend werden alle entdeckten CWEs im Programm „Chess Online mit einer kurzen Begründung für das Auftreten aufgezählt. Einrückungen stellen eine Eltern-Kind-Beziehung der CWEs dar, wobei Kind-CWEs nur bei einem Elternteil aufgezählt werden. Die Untergliederung entspricht der Aufteilung nach Forschungskonzepten („Research Concepts“) der MITRE Corporation. CWEs der Klasse „Pillar“, welche die oberste Gliederungsebene darstellen, sind **fett** geschrieben, während CWEs mit Kind-CWEs unterstrichen sind. Grüne CWEs wurden in der schwachen Version entdeckt und anschließend in der starken Version behoben. Alle CWEs mit detaillierten Informationen lassen sich auf der Website der Common Weakness Enumeration nachschlagen.

CWE-Website: (https://cwe.mitre.org/) [aufgerufen am 2.1.2023]

Gefundene CWE: 106

Davon behoben: 49 (≈ 46,2%)

- **CWE-284: Improper Access Control**
  - CWE-287: Improper Authentication
  - CWE-1390: Weak Authentication
    - CWE-262: Not Using Password Aging
      - CWE-290: Authentication Bypass by Spoofing
      - CWE-294: Authentication Bypass by Capture-replay
      - CWE-307: Improper Restriction of Excessive Authentication Attempts
      - CWE-308: Use of Single-factor Authentication
      - CWE-309: Use of Password System for Primary Authentication
    - CWE-522: Insufficiently Protected Credentials
      - CWE-256: Plaintext Storage of a Password
      - CWE-257: Storing Passwords in a Recoverable Format
      - CWE-523: Unprotected Transport of Credentials
      - CWE-549: Missing Password Field Masking
    - CWE-1391: Use of Weak Credentials
      - CWE-521: Weak Password Requirements
      - CWE-798: Use of Hard-coded Credentials
        - CWE-259: Use of Hard-coded Password
  - CWE-923: Improper Restriction of Communication Channel to Intended Endpoints
    - CWE-300: Channel Accessible by Non-Endpoint

CWE-664: Improper Control of a Resource Through its Lifetime

- CWE-1329: Reliance on Component That is Not Updateable
  - CWE-1277: Firmware Not Updateable
- CWE-221: Information Loss or Omission
  - CWE-223: Omission of Security-relevant Information
    - CWE-778: Insufficient Logging
- CWE-400: Uncontrolled Resource Consumption
  - CWE-770: Allocation of Resources Without Limits or Throttling
- CWE-405: Asymmetric Resource Consumption (Amplification)
  - CWE-1050: Excessive Platform Resource Consumption within a Loop
  - CWE-1072: Data Resource Access without Use of Connection Pooling
  - CWE-1084: Invokable Control Element with Excessive File or Data Access Operations
  - CWE-1176: Inefficient CPU Computation
    - CWE-1046: Creation of Immutable Text Using String Concatenation
    - CWE-1067: Excessive Execution of Sequential Searches of Data Resource
  - CWE-406: Insufficient Control of Network Message Volume (Network Amplification)
- CWE-410: Insufficient Resource Pool
- CWE-662: Improper Synchronization
  - CWE-667: Improper Locking
    - CWE-413: Improper Resource Locking

CWE-591: Sensitive Data Storage in Improperly Locked Memory

CWE-820: Missing Synchronization

CWE-668: Exposure of Resource to Wrong Sphere

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

CWE-203: Observable Discrepancy

CWE-208: Observable Timing Discrepancy

CWE-359: Exposure of Private Personal Information to an Unauthorized Actor

CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory

CWE-540: Inclusion of Sensitive Information in Source Code

CWE-913: Improper Control of Dynamically-Managed Code Resources

CWE-502: Deserialization of Untrusted Data

CWE-922: Insecure Storage of Sensitive Information

CWE-312: Cleartext Storage of Sensitive Information

CWE-691: Insufficient Control Flow Management

CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

CWE-366: Race Condition within a Thread

CWE-431: Missing Handler

CWE-674: Uncontrolled Recursion

CWE-705: Incorrect Control Flow Scoping

CWE-248: Uncaught Exception

CWE-799: Improper Control of Interaction Frequency

CWE-834: Excessive Iteration

CWE-94: Improper Control of Generation of Code ('Code Injection')

CWE-693: Protection Mechanism Failure

- CWE-311: Missing Encryption of Sensitive Data
  - CWE-319: Cleartext Transmission of Sensitive Information
- CWE-330: Use of Insufficiently Random Values
  - CWE-1241: Use of Predictable Algorithm in Random Number Generator
  - CWE-331: Insufficient Entropy
  - CWE-334: Small Space of Random Values
  - CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
- CWE-345: Insufficient Verification of Data Authenticity
  - CWE-1293: Missing Source Correlation of Multiple Independent Data
  - CWE-353: Missing Support for Integrity Check (telnet integrity?)
  - CWE-354: Improper Validation of Integrity Check Value
  - CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel
- CWE-358: Improperly Implemented Security Check for Standard
- CWE-654: Reliance on a Single Factor in a Security Decision

CWE-707: Improper Neutralization

- CWE-138: Improper Neutralization of Special Elements
  - CWE-149: Improper Neutralization of Quoting Syntax
  - CWE-151: Improper Neutralization of Comment Delimiters
  - CWE-159: Improper Handling of Invalid Use of Special Elements
    - CWE-167: Improper Handling of Additional Special Element
  - CWE-162: Improper Neutralization of Trailing Special Elements
  - CWE-790: Improper Filtering of Special Elements
- CWE-20: Improper Input Validation
  - CWE-1286: Improper Validation of Syntactic Correctness of Input
- CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
  - CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)
  - CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')
  - CWE-943: Improper Neutralization of Special Elements in Data Query Logic
    - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

CWE-710: Improper Adherence to Coding Standards

- CWE-1041: Use of Redundant Code
- CWE-1059: Insufficient Technical Documentation
  - CWE-1118: Insufficient Documentation of Error Handling Techniques
- CWE-1076: Insufficient Adherence to Expected Conventions
  - CWE-1078: Inappropriate Source Code Style or Formatting
    - CWE-1099: Inconsistent Naming Conventions for Identifiers
- CWE-1120: Excessive Code Complexity
  - CWE-1047: Modules with Circular Dependencies
  - CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses
  - CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters
  - CWE-1080: Source Code File with Excessive Number of Lines of Code
  - CWE-1124: Excessively Deep Nesting