# CWE: Common Weakness Enumeration

Table 1 shows the 20 most frequent Weaknesses that have appeared in the CVE database.

|  |  |
| --- | --- |
| 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 6593 |
| 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 6377 |
| 264-Permissions | 4477 |
| 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 4132 |
| 20-Improper Input Validation | 3665 |
| 399-Resource Management Errors | 2648 |
| 200-Information Exposure | 2481 |
| 310-Cryptographic Issues | 2233 |
| 94-Improper Control of Generation of Code ('Code Injection') | 2063 |
| 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 1848 |
| 189-Numeric Errors | 1288 |
| 352-Cross-Site Request Forgery (CSRF) | 1118 |
| 287-Improper Authentication | 976 |
| 255-Credentials Management | 583 |
| 59-Improper Link Resolution Before File Access ('Link Following') | 421 |
| 362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 353 |
| 16-Configuration | 277 |
| 284-Improper Access Control | 200 |
| 78-Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 194 |
| 134-Uncontrolled Format String | 162 |
| 17-Code | 157 |

Taking time into account, we can see that before 1995, CWE was not reported with CVE. However, since then, 119, 20, 264, etc. have been consistently present in the top 10, indicating that some categories of vulnerability are either not easily fixed or recurs over time.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Until 2001 | | | Until 2006 | | Until 2011 | | Until 2016 | |
| 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 15 | 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | | 334 | 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 3091 | 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 3487 |
| 20-Improper Input Validation | 11 | 94-Improper Control of Generation of Code ('Code Injection') | | 232 | 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 3000 | 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 3156 |
| 264-Permissions | 10 | 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | | 220 | 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 2757 | 264-Permissions | 2581 |
| 16-Configuration | 8 | 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | | 169 | 264-Permissions | 1735 | 20-Improper Input Validation | 1941 |
| 94-Improper Control of Generation of Code ('Code Injection') | 7 | 264-Permissions | | 151 | 20-Improper Input Validation | 1573 | 310-Cryptographic Issues | 1905 |
| 200-Information Exposure | 7 | 20-Improper Input Validation | | 140 | 94-Improper Control of Generation of Code ('Code Injection') | 1300 | 200-Information Exposure | 1501 |
| 310-Cryptographic Issues | 5 | 399-Resource Management Errors | | 121 | 399-Resource Management Errors | 1266 | 399-Resource Management Errors | 1260 |
| 59-Improper Link Resolution Before File Access ('Link Following') | 4 | 200-Information Exposure | | 90 | 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 1208 | 89-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 872 |
| 255-Credentials Management | 4 | 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | | 74 | 200-Information Exposure | 883 | 352-Cross-Site Request Forgery (CSRF) | 758 |
| 287-Improper Authentication | 4 | 189-Numeric Errors | | 57 | 189-Numeric Errors | 691 | 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 563 |

Here are the items that repeatedly occur in every time bin:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | 2001 | 2006 | 2011 | 2016 |
| 119-Improper Restriction of Operations within the Bounds of a Memory Buffer | 15 | 334 | 2757 | 3487 |
| 79-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 1 | 220 | 3000 | 3156 |
| 264-Permissions | 10 | 151 | 1735 | 2581 |
| 20-Improper Input Validation | 11 | 140 | 1573 | 1941 |
| 94-Improper Control of Generation of Code ('Code Injection') | 7 | 232 | 1300 | 524 |
| 200-Information Exposure | 7 | 90 | 883 | 1501 |
| 399-Resource Management Errors | 1 | 121 | 1266 | 1260 |
| 310-Cryptographic Issues | 5 | 23 | 300 | 1905 |
| 22-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 3 | 74 | 1208 | 563 |
| 16-Configuration | 8 | 28 | 172 | 69 |
| 287-Improper Authentication | 4 | 35 | 549 | 388 |
| 255-Credentials Management | 4 | 28 | 229 | 322 |
| 59-Improper Link Resolution Before File Access ('Link Following') | 4 | 13 | 286 | 118 |
| 362-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | 2 | 13 | 116 | 222 |

This table is sorted by a special index that calculate the average ranking among the groups:

# CAPEC: Attack Pattern

Here is the CAPEC over all time ranked by frequency (top 20)

|  |  |  |
| --- | --- | --- |
| ID | Name | Frequency |
| 8 | Buffer Overflow in an API Call | 10342 |
| 9 | Buffer Overflow in Local Command-Line Utilities | 10342 |
| 10 | Buffer Overflow via Environment Variables | 10342 |
| 42 | MIME Conversion | 10342 |
| 24 | Filter Failure through Buffer Overflow | 10342 |
| 14 | Client-side Injection-induced Buffer Overflow | 10342 |
| 45 | Buffer Overflow via Symbolic Links | 10342 |
| 46 | Overflow Variables and Tags | 10342 |
| 47 | Buffer Overflow via Parameter Expansion | 10342 |
| 106 | Cross Site Scripting through Log Files | 10117 |
| 91 | XSS in IMG Tags | 10117 |
| 86 | Embedding Script (XSS) in HTTP Headers | 10098 |
| 32 | Embedding Scripts in HTTP Query Strings | 10098 |
| 244 | Cross-Site Scripting via Encoded URI Schemes | 10098 |
| 18 | Embedding Scripts in Non-Script Elements | 10098 |
| 85 | AJAX Fingerprinting | 10098 |
| 63 | Simple Script Injection | 10098 |
| 199 | Cross-Site Scripting Using Alternate Syntax | 10098 |
| 79 | Using Slashes in Alternate Encoding | 8134 |
| 108 | Command Line Execution through SQL Injection | 8069 |

Dividing those into four time bins:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Until 2001 | | | Until 2006 | | | Until 2011 | | | Until 2016 | | |
| 8 | Buffer Overflow in an API Call | 26 | 45 | Buffer Overflow via Symbolic Links | 476 | 108 | Command Line Execution through SQL Injection | 4769 | 47 | Buffer Overflow via Parameter Expansion | 5459 |
| 9 | Buffer Overflow in Local Command-Line Utilities | 26 | 47 | Buffer Overflow via Parameter Expansion | 476 | 7 | Blind SQL Injection | 4715 | 42 | MIME Conversion | 5459 |
| 10 | Buffer Overflow via Environment Variables | 26 | 24 | Filter Failure through Buffer Overflow | 476 | 109 | Object Relational Mapping Injection | 4715 | 8 | Buffer Overflow in an API Call | 5459 |
| 14 | Client-side Injection-induced Buffer Overflow | 26 | 46 | Overflow Variables and Tags | 476 | 110 | SQL Injection through SOAP Parameter Tampering | 4715 | 9 | Buffer Overflow in Local Command-Line Utilities | 5459 |
| 45 | Buffer Overflow via Symbolic Links | 26 | 14 | Client-side Injection-induced Buffer Overflow | 476 | 66 | SQL Injection | 4715 | 10 | Buffer Overflow via Environment Variables | 5459 |
| 42 | MIME Conversion | 26 | 42 | MIME Conversion | 476 | 244 | Cross-Site Scripting via Encoded URI Schemes | 4622 | 14 | Client-side Injection-induced Buffer Overflow | 5459 |
| 46 | Overflow Variables and Tags | 26 | 10 | Buffer Overflow via Environment Variables | 476 | 106 | Cross Site Scripting through Log Files | 4622 | 45 | Buffer Overflow via Symbolic Links | 5459 |
| 24 | Filter Failure through Buffer Overflow | 26 | 9 | Buffer Overflow in Local Command-Line Utilities | 476 | 91 | XSS in IMG Tags | 4622 | 24 | Filter Failure through Buffer Overflow | 5459 |
| 47 | Buffer Overflow via Parameter Expansion | 26 | 8 | Buffer Overflow in an API Call | 476 | 86 | Embedding Script (XSS) in HTTP Headers | 4622 | 46 | Overflow Variables and Tags | 5459 |
| 22 | Exploiting Trust in Client | 22 | 91 | XSS in IMG Tags | 361 | 85 | AJAX Fingerprinting | 4622 | 106 | Cross Site Scripting through Log Files | 5122 |

Too many items in CAPEC repeatedly shows itself through all time. Here are some most frequent CAPEC entries:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Name | Until 2001 | Until 2006 | Until 2011 | Until 2016 |
| 8 | Buffer Overflow in an API Call | 26 | 476 | 4381 | 5459 |
| 9 | Buffer Overflow in Local Command-Line Utilities | 26 | 476 | 4381 | 5459 |
| 10 | Buffer Overflow via Environment Variables | 26 | 476 | 4381 | 5459 |
| 14 | Client-side Injection-induced Buffer Overflow | 26 | 476 | 4381 | 5459 |
| 24 | Filter Failure through Buffer Overflow | 26 | 476 | 4381 | 5459 |
| 42 | MIME Conversion | 26 | 476 | 4381 | 5459 |
| 45 | Buffer Overflow via Symbolic Links | 26 | 476 | 4381 | 5459 |
| 46 | Overflow Variables and Tags | 26 | 476 | 4381 | 5459 |
| 47 | Buffer Overflow via Parameter Expansion | 26 | 476 | 4381 | 5459 |
| 91 | XSS in IMG Tags | 12 | 361 | 4622 | 5122 |
| 106 | Cross Site Scripting through Log Files | 12 | 361 | 4622 | 5122 |
| 18 | Embedding Scripts in Non-Script Elements | 12 | 361 | 4622 | 5103 |
| 32 | Embedding Scripts in HTTP Query Strings | 12 | 361 | 4622 | 5103 |
| 63 | Simple Script Injection | 12 | 361 | 4622 | 5103 |
| 85 | AJAX Fingerprinting | 12 | 361 | 4622 | 5103 |
| 86 | Embedding Script (XSS) in HTTP Headers | 12 | 361 | 4622 | 5103 |
| 199 | Cross-Site Scripting Using Alternate Syntax | 12 | 361 | 4622 | 5103 |
| 244 | Cross-Site Scripting via Encoded URI Schemes | 12 | 361 | 4622 | 5103 |
| 79 | Using Slashes in Alternate Encoding | 21 | 307 | 3730 | 4076 |
| 22 | Exploiting Trust in Client | 22 | 268 | 3076 | 3884 |

This shows many attack patterns are persistent over time. Some old attack patterns could still be very effective. This is possibly related to how some CWE entries also persists over time. Similar weaknesses are likely to be exploited by the same attack pattern.

# CPE: Platform

CPE is an enumeration of platforms, and originally each entry has a version associated with it, so that different versions of the same platform will be treated as individual platforms. In order to comprehensively understand the evolution of vulnerability associated with platforms, we did the analysis with the original entries, and also with entries where versions are merged. If one CVE affects several versions of the same platform, the frequency will be counted as “1”.

First, the overall most frequent platforms are presented in the following tables. Google Chrome dominates the table of version specific analysis, but ranked 17 in version-merged analysis. It shows that vulnerabilities affecting Google Chrome is consistent throughout each version. The same vulnerabilities are mostly inherited by the next version, and few new vulnerabilities appear. It could also be caused by the fact that Google Chrome provides more frequent version updates. In such a case, version-merged analysis would provide better insights.

|  |  |
| --- | --- |
| ID | Frequency |
| mozilla:firefox | 21315 |
| mozilla:thunderbird | 15959 |
| mozilla:seamonkey | 15875 |
| sun:jre | 7842 |
| sun:jdk | 7333 |
| adobe:flash\_player | 5637 |
| adobe:acrobat | 4894 |
| adobe:acrobat\_reader | 4627 |
| oracle:jdk | 3337 |
| oracle:jre | 3267 |
| apple:mac\_os\_x | 3199 |
| adobe:adobe\_air | 2817 |
| apple:iphone\_os | 2699 |
| linux:linux\_kernel | 2321 |
| microsoft:windows\_server\_2008 | 2290 |
| apple:mac\_os\_x\_server | 2245 |
| google:chrome | 2000 |
| sun:sdk | 1935 |
| cisco:ios | 1761 |
| microsoft:windows\_xp | 1761 |

|  |  |
| --- | --- |
| ID | Frequency |
| google:chrome:1.0.154.53 | 513 |
| google:chrome:1.0.154.59 | 510 |
| mozilla:firefox:1.0 | 509 |
| google:chrome:2.0.172.30 | 506 |
| google:chrome:2.0.172.33 | 506 |
| google:chrome:2.0.172.37 | 505 |
| google:chrome:2.0.172.28 | 503 |
| google:chrome:2.0.172.27 | 502 |
| google:chrome:2.0.172.2 | 502 |
| google:chrome:2.0.170.0 | 502 |
| google:chrome:2.0.169.1 | 502 |
| google:chrome:2.0.169.0 | 502 |
| google:chrome:2.0.172.38 | 502 |
| google:chrome:2.0.172.8 | 502 |
| google:chrome:3.0.182.2 | 502 |
| google:chrome:1.0.154.65 | 502 |
| google:chrome:3.0.195.33 | 495 |
| google:chrome:3.0.190.2 | 494 |
| google:chrome:1.0.154.43 | 488 |
| google:chrome:1.0.154.36 | 488 |

Table 2 shows the frequencies of CPE over different time intervals. It can be seen that CPE entries change over time. Sun Solaris was the number one frequent CPE from until 2001, but it was not in top 10 in the following years. Mozilla on the other hand became the main source of CVE after 2002. From another point of view, platforms recorded in CVE were mostly operating systems before 2006, and afterwards application-related platforms, such as jdk, firefox, acrobat, etc. started to rise.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Until 2001 | | | Until 2006 | | | Until 2011 | | | Until 2016 | | |
| Platform ID | Frequency | Percentage | Platform ID | Frequency | Percentage | Platform ID | Frequency | Percentage | Platform ID | Frequency | Percentage |
| sun:solaris | 353 | 4.92% | microsoft:windows\_2000 | 895 | 2.31% | mozilla:firefox | 5858 | 6.92% | mozilla:firefox | 14742 | 10.82% |
| redhat:linux | 268 | 3.73% | mozilla:firefox | 715 | 1.84% | mozilla:thunderbird | 4439 | 5.24% | mozilla:seamonkey | 11401 | 8.37% |
| hp:hp-ux | 210 | 2.93% | microsoft:windows\_xp | 708 | 1.82% | mozilla:seamonkey | 4313 | 5.09% | mozilla:thunderbird | 11151 | 8.18% |
| microsoft:windows\_nt | 205 | 2.86% | microsoft:windows\_nt | 705 | 1.82% | sun:jre | 3904 | 4.61% | adobe:flash\_player | 4646 | 3.41% |
| sgi:irix | 200 | 2.79% | linux:linux\_kernel | 680 | 1.75% | sun:jdk | 3355 | 3.96% | sun:jdk | 3856 | 2.83% |
| ibm:aix | 192 | 2.68% | apple:mac\_os\_x | 661 | 1.70% | adobe:acrobat | 2042 | 2.41% | sun:jre | 3785 | 2.78% |
| freebsd:freebsd | 190 | 2.65% | suse:suse\_linux | 613 | 1.58% | sun:sdk | 1909 | 2.25% | oracle:jdk | 3325 | 2.44% |
| sun:sunos | 133 | 1.85% | microsoft:windows\_2003\_server | 602 | 1.55% | adobe:acrobat\_reader | 1904 | 2.25% | oracle:jre | 3253 | 2.39% |
| microsoft:windows\_2000 | 127 | 1.77% | apple:mac\_os\_x\_server | 592 | 1.53% | apple:mac\_os\_x | 1433 | 1.69% | adobe:acrobat | 2811 | 2.06% |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Until 2001 | | | Until 2006 | | | Until 2011 | | | Until 2016 | | |
| microsoft:windows\_nt:4.0 | 95 | 0.67% | microsoft:ie:6.0 | 156 | 0.12% | google:chrome:1.0.154.53 | 418 | 0.04% | microsoft:internet\_explorer:10 | 414 | 0.05% |
| microsoft:windows\_2000 | 83 | 0.58% | linux:linux\_kernel:2.6.0 | 154 | 0.12% | google:chrome:1.0.154.59 | 415 | 0.04% | microsoft:internet\_explorer:9 | 409 | 0.05% |
| sun:solaris:2.5.1 | 81 | 0.57% | linux:linux\_kernel:2.6.1 | 136 | 0.11% | google:chrome:2.0.172.33 | 411 | 0.04% | microsoft:internet\_explorer:11:- | 370 | 0.04% |
| sun:solaris:2.5 | 73 | 0.51% | linux:linux\_kernel:2.6.3 | 133 | 0.11% | google:chrome:2.0.172.30 | 411 | 0.04% | microsoft:internet\_explorer:8 | 316 | 0.04% |
| sun:solaris:2.6 | 73 | 0.51% | linux:linux\_kernel:2.6.5 | 133 | 0.11% | google:chrome:2.0.172.37 | 410 | 0.04% | mozilla:seamonkey:2.0.10 | 289 | 0.03% |
| sun:solaris:2.4 | 66 | 0.46% | linux:linux\_kernel:2.6.4 | 132 | 0.10% | google:chrome:2.0.172.28 | 408 | 0.04% | mozilla:seamonkey:2.0:rc1 | 289 | 0.03% |
| sun:solaris:7.0 | 62 | 0.44% | linux:linux\_kernel:2.6.6 | 130 | 0.10% | google:chrome:1.0.154.65 | 407 | 0.04% | mozilla:seamonkey:2.0:rc2 | 289 | 0.03% |
| microsoft:internet\_information\_server:4.0 | 60 | 0.42% | linux:linux\_kernel:2.6.7 | 129 | 0.10% | google:chrome:2.0.172.27 | 407 | 0.04% | mozilla:seamonkey:2.1:alpha3 | 289 | 0.03% |
| sun:solaris:2.5.1::x86 | 58 | 0.41% | linux:linux\_kernel:2.6.2 | 128 | 0.10% | google:chrome:2.0.172.2 | 407 | 0.04% | mozilla:seamonkey:2.1:alpha2 | 289 | 0.03% |

Table 3 shows CPEs that have appear in all time intervals, ranked in top 50s. Without the limit of top 50, there are many entries; however, most of them are trivial cases, as the frequency is too small. Two entries appear when versions are merged; no entry appear when versions are counted specifically. Not surprisingly, it shows that CPEs are not consistent over time.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Until Year | 2001 | 2006 | 2011 | 2016 |
| cisco:ios | 51 | 183 | 791 | 736 |
| linux:linux\_kernel | 80 | 680 | 962 | 599 |