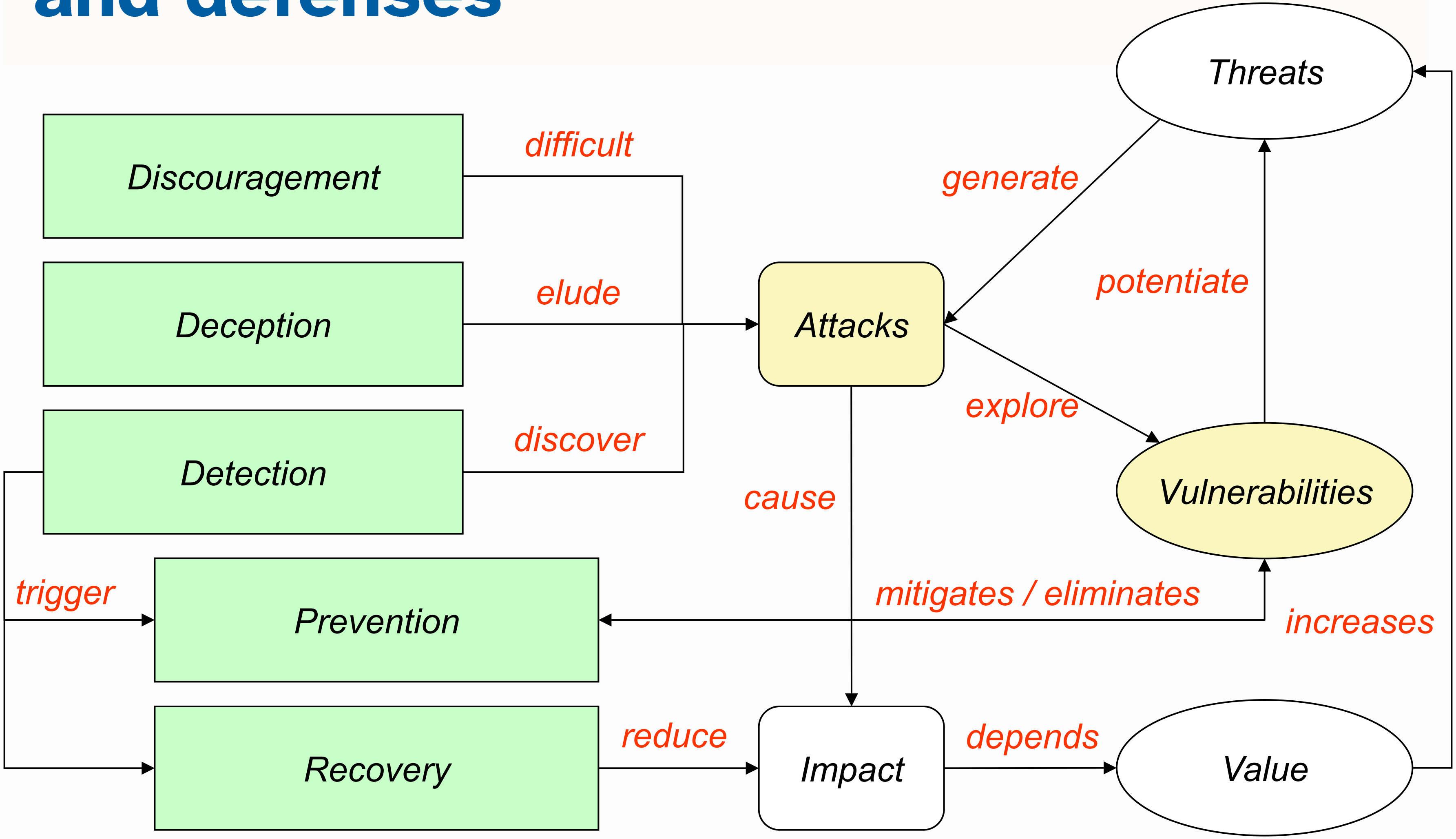
Vulnerabilities

Vulnerabilities, attacks, threats, risks and defenses



Risk

Risk = Impact × Probability of a successful attack

- High impact & probability → high risk

- Low impact → low risk
- Low probability → low risk

- Therefore, to reduce risk we need to reduce one of them
  - Or both

Impact: material (tangible consequences)

- Financial losses
  - Theft of funds
    - e.g., through ransomware or fraudulent transfers
  - Loss of revenue due to operational downtime
  - Costs related to incident response, recovery, and forensic analysis
  - Legal fines and regulatory penalties
    - e.g., GDPR fines
  - Increased insurance premiums or loss of coverage
- Operational disruption
  - IT systems and networks may be taken offline
  - Production halts in manufacturing or logistics
  - Disruption of services
    - e.g., healthcare, transport, banking, etc.

Impact: material (tangible consequences)

- Data loss or corruption
  - Loss of critical data
    - Client records, IP, source code, etc.
  - Inability to recover data due to lack of backups or encryption
  - Corruption of operational or strategic data
- Damage to infrastructure
  - Physical damage
    - In rare cases, like Stuxnet or cyber-physical attacks
  - Loss of control over industrial control systems or IoT devices
- Increased security and recovery costs
  - Investment in new cybersecurity tools and systems
  - Hiring consultants or rebuilding infrastructure

Impact: immaterial (intangible consequences)

- Reputation damage
  - Loss of customer trust
  - Damage to brand image or credibility
  - Negative media coverage and public perception
- Legal and regulatory impact
  - Legal liability for leaked or mishandled personal data
  - Breach of contract or SLA obligations
- Loss of intellectual property
  - Theft of trade secrets, product designs, or source code
  - Competitive disadvantage if leaked to rivals

Impact: immaterial (intangible consequences)

- Loss of customer or partner confidence
  - Termination of business partnerships
  - Customer churn or lost future opportunities
- Psychological and social impact
  - Stress and burnout among employees
  - Fear and confusion among customers or citizens
  - Erosion of digital trust in society
- National security and geopolitical tensions
  - Espionage, sabotage, or acts of cyberwarfare
  - Destabilization of public trust in critical institutions
    - Elections, utilities, etc.

Measures (and some tools)

- Discouragement
  - Punishment
    - Legal restrictions
    - Forensic evidences
  - Security barriers
    - Firewalls
    - Autentication
    - Secure communication
    - Sandboxing (containers et al.)
- Detection
  - Intrusion detection system
    - e.g. Snort, Zeek, Suricata
  - Auditing
  - Forensic break-in analysis
- Deception
  - Honeypots / honeynets
  - Forensic follow-up
- Prevention
  - Restrictive policies
    - e.g. least privilege principle
  - Vulnerability scanning
    - e.g. OpenVAS, Metasploit
  - Vulnerability patching
    - e.g. regular updates
- Recovery
  - Backups
  - Redundant systems
  - Forensic recovery

Vulnerability management: from the Morris Worm to CERT/CC

- The 1988 Morris Worm was one of the first computer worms distributed via the internet
  - And it had significant impact
- Infected systems
  - Estimated 6,000 to 10,000 computers
  - Roughly 10% of the ~60,000 machines on the Internet at the time
- Downtime
  - Affected systems were rendered slow or unusable for days, as administrators worked to identify, contain, and clean the infection

Vulnerability management: from the Morris Worm to CERT/CC

- Computer Emergency Response Team / Coordination Center
  - Created in 1988, at CMU, in the aftermath of the Morris Worm
  - The worm highlighted the need for a centralized body to coordinate responses to cybersecurity incidents and help organizations mitigate vulnerabilities

- CERT/CC was established as a resource for identifying, managing, and disseminating information about cyber threats
  - Thus promoting proactive measures to improve overall Internet security

- It became the first global, centralized entity to track and respond to computer security vulnerabilities and incidents.

Common Vulnerabilities and Exposures (CVE)

- Dictionary of publicly known information security vulnerabilities and exposures (https://www.cve.org/)
  - For vulnerability management
  - For patch management
  - For vulnerability alerting
  - For intrusion detection
- Uses common identifiers for the same CVEs
  - Enable data exchange between security products
  - Provide a baseline index point for evaluating coverage of tools and services
- Details about a vulnerability can be kept private
  - Part of responsible disclosure: until owner provides a fix

Vulnerability

A mistake in software that can be directly used by an attacker to gain access to a system or network

- A mistake is a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system
  - This excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system

- A CVE vulnerability is a state in a computing system (or set of systems) that either:
  - Allows an attacker to execute commands as another user
  - Allows an attacker to access data that is contrary to the specified access restrictions for that data
  - Allows an attacker to pose as another entity
  - Allows an attacker to conduct a denial of service

Exposure

A configuration issue or a mistake in software allowing access to information or capabilities used as a stepping-stone into a system or network

- A configuration issue or a mistake is an exposure if it does not directly allow compromise
  - But could be an important component of a successful attack, and is a violation of a reasonable security policy
- An CVE exposure describes a state in a computing system (or set of systems) that is not a vulnerability, but either:
  - Allows an attacker to conduct information gathering activities
  - Allows an attacker to hide activities
  - Includes a capability that behaves as expected, but can be easily compromised
  - Is a primary point of entry that an attacker may attempt to use to gain access to the system or data
  - Is considered a problem by some reasonable security policy

CVE identifiers

- Aka CVE names, CVE numbers, CVE-IDs, CVEs

- Unique, common identifiers for publicly known information security vulnerabilities
  - Have "candidate" or "entry" status
  - Candidate: under review for inclusion in the list
  - Entry: accepted to the CVE List

- Format
  - CVE identifier number (CVE-Year-Order)
  - Status (Candidate or Entry)
  - Brief description of the vulnerability or exposure
  - References to extra information

CVE severity score

- Indicates a CVE impact and urgency
  - Calculated using the Common Vulnerability Scoring System (CVSS)
- CVSS
  - Assigns a score from 0 to 10

    https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
  - Uses factors like:
    - Exploitability
    - Impact on confidentiality, integrity, availability

CVSS scores

- 0.0 – 3.9: Low severity
  - Minor risk, unlikely to be exploited
- 4.0 – 6.9: Medium severity
  - Moderate risk, may require specific conditions
- 7.0 – 8.9: High severity
  - Serious risk, could be exploited easily
- 9.0 – 10.0: Critical severity
  - Very high risk, urgent patch needed

Vulnerability detection

- Specific tools can detect vulnerabilities
  - Exploiting known vulnerabilities
  - Testing known vulnerability patterns
    - e.g., buffer overflow, SQL injection, XSS, etc.
- Specific tools can replicate known attacks
  - Use known exploits for known vulnerabilities
    - e.g.: MS Samba v1 exploit used by WannaCry
  - Can be used to implement countermeasures
- Vital to assert the robustness of production systems and applications
  - Service often provided by third-party companies

Vulnerability detection

- Can be applied to:
  - Source code (static analysis)
    - OWASP LAPSE+, RIPS, Veracode, …
  - Running application (dynamic analysis)
    - Valgrind, HCL AppScan, GCC, …
  - Externally as a remote client:
    - OpenVAS, Metasploit, …

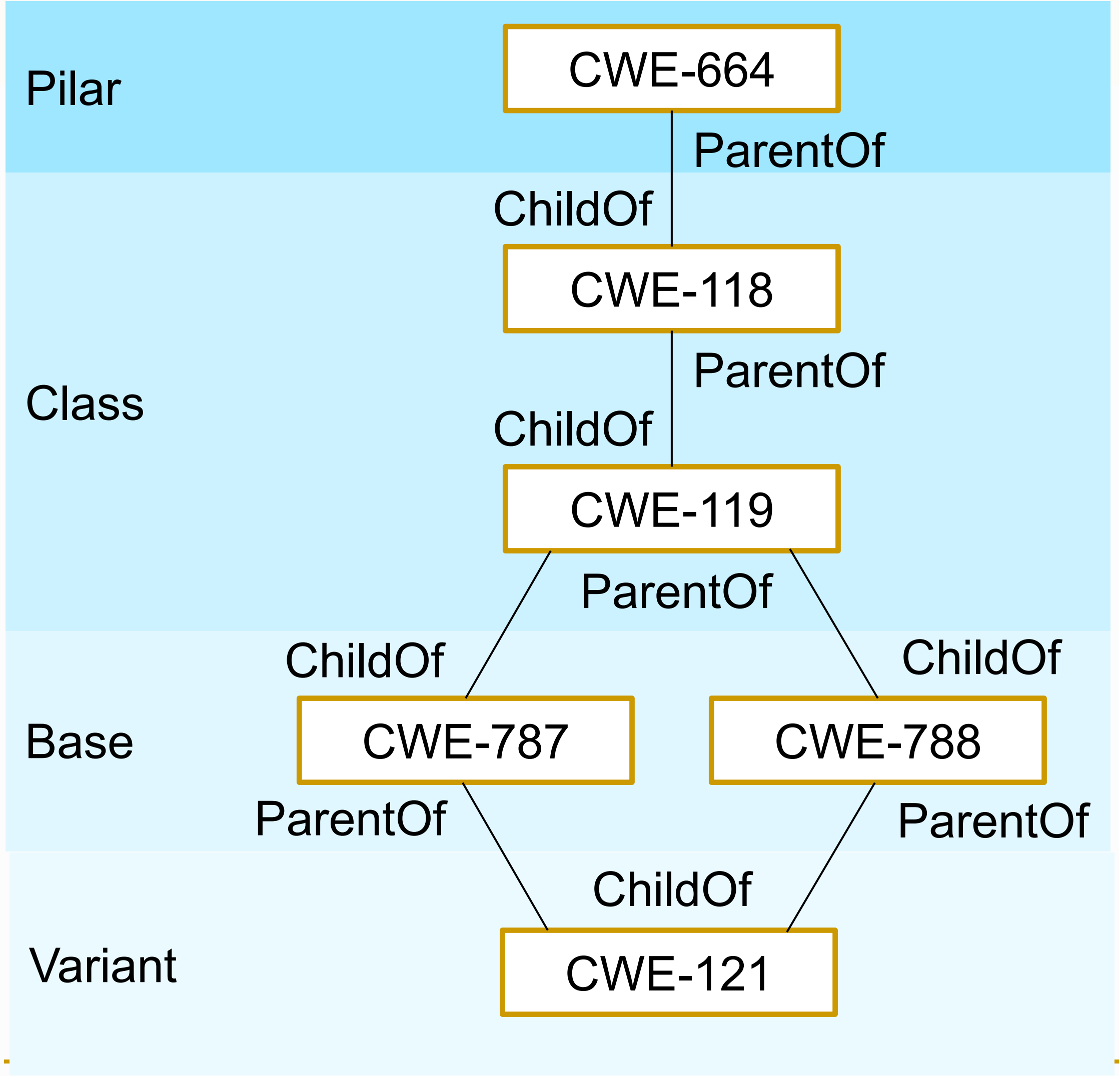
- Should not be blindly applied to production systems!
  - Potential data loss/corruption
  - Potential DoS
  - Potential illegal activity

Common Weakness Enumeration (CWE)

- Common language of discourse for discussing, finding and dealing with the causes of software security vulnerabilities
  - Found in code, design, or system architecture
  - Each individual CWE represents a single vulnerability type
  - Currently maintained by the MITRE Corporation
    - A detailed CWE list is currently available at the MITRE website
  - The list provides a detailed definition for each individual CWE

- Individual CWEs are held within a hierarchical structure
  - CWEs at higher levels provide a broad overview of a vulnerability type
    - Can have many children CWEs associated with them
  - CWEs at deeper levels provide a finer granularity
    - Usually have fewer or no children CWEs

CWE hierarchies



Pilar

CWE-664

ParentOf

ChildOf

Class

CWE-118

ParentOf

ChildOf

CWE-119

ParentOf

ChildOf

ChildOf

Base

CWE-787

CWE-788

ParentOf

ParentOf

ChildOf

Variant

CWE-121

Improper Control of a Resource Through its Lifetime

Incorrect Access of Indexable Resource ('Range Error')

Improper Restriction of Operations within the Bounds of a Memory Buffer

Out-of-bounds Write

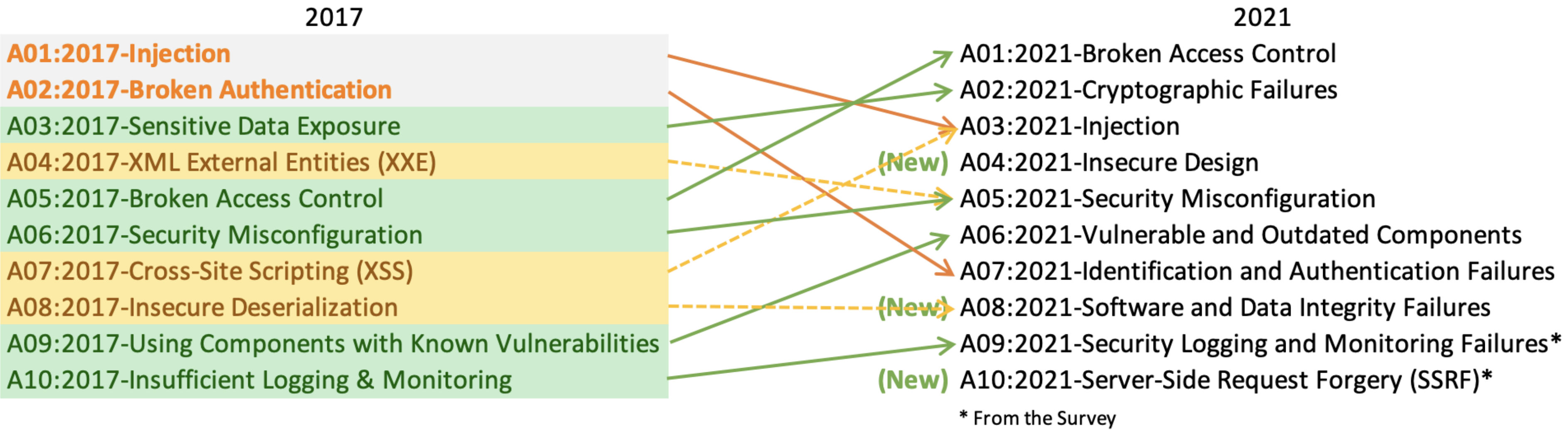
Access of Memory Location After End of Buffer

Stack-based Buffer Overflow

CWE mappings:
OWASP Top 10 (2021, Web)

1. Broken Access control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

OWASP Top 10 evolution



2017

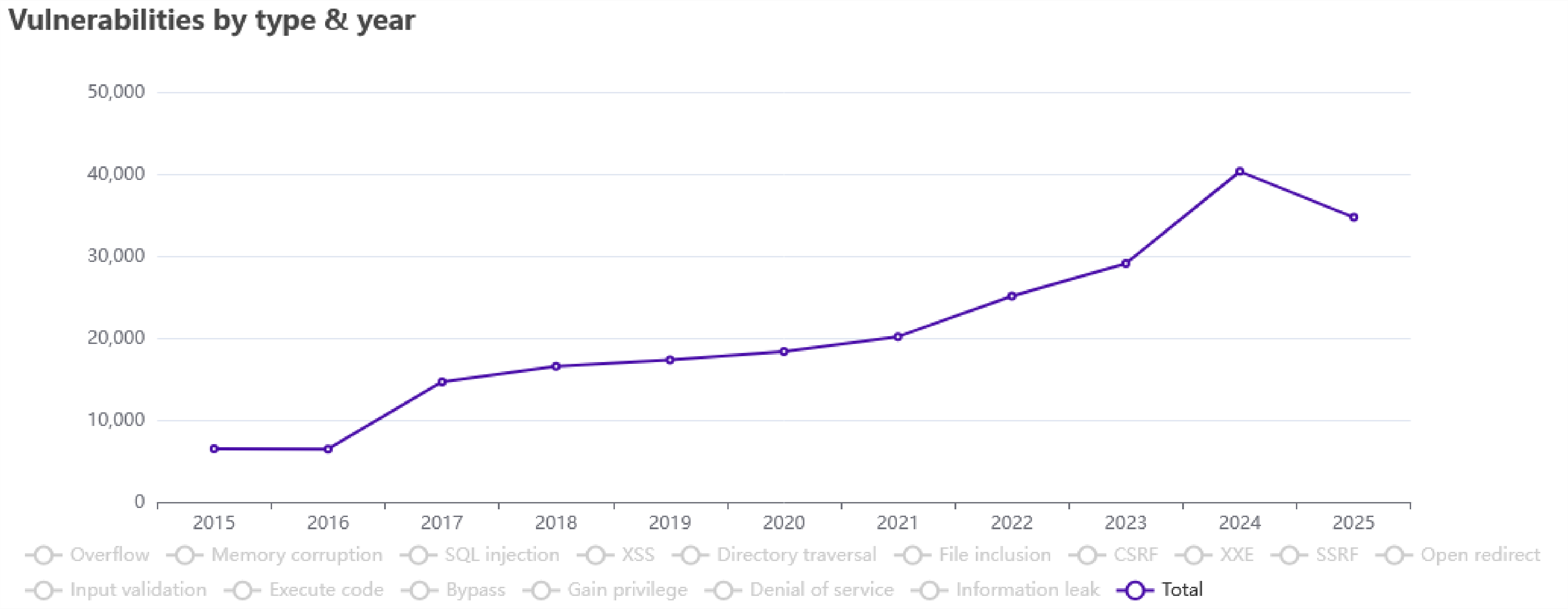
- A01:2017-Injection
- A02:2017-Broken Authentication
- A03:2017-Sensitive Data Exposure
- A04:2017-XML External Entities (XXE)
- A05:2017-Broken Access Control
- A06:2017-Security Misconfiguration
- A07:2017-Cross-Site Scripting (XSS)
- A08:2017-Insecure Deserialization
- A09:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- (New) A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- (New) A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- (New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

CVEs per year – cvedetails.com



Zero Day (or Zero Hour) Attack / Threat

- Attack using vulnerabilities which are:
  - Unknown to others
  - Undisclosed to the software vendor
- Occurs at the day zero of the knowledge about those vulnerabilities
  - For which no security fix is available
- A single “day zero” may exist for months/years
  - Known to attackers, unknown to others
  - Frequently part of attack arsenal
  - Traded around in specific markets

Computer Emergency Response Team (CERT)

- Organization primarily concerned with coordinating responses and providing expert advice during cyber emergencies
  - Incident coordination during an emergency
    - May operate in a national or organizational context
  - Public disclosure of vulnerabilities
    - e.g. Zero-day vulnerabilities
  - Advisories and warnings
- CERT/CC (Coordination Center) @ CMU
  - The top component of the large CERT Program

Computer Security Incident Response Team (CSIRT)

- An organization more broadly focused on managing a full range of cybersecurity incidents, not just emergencies
  - Incident detection and initial triage
  - Investigation and analysis of incidents
  - Long-term security improvement through lessons learned
  - Regular monitoring and forensics
  - Collaboration with external stakeholders
    - e.g., other CSIRTs, vendors, or governmental bodies

Portuguese CERTs / CSIRTs

- CERT.PT
  - https://www.cncs.gov.pt/pt/certpt/
- National CSIRT Network
  - https://www.redecsirt.pt
- CSIRT @ UA
  - https://csirt.ua.pt

Security alerts & activity trends

- Vital to the fast dissemination of knowledge about new vulnerabilities
  - US-CERT Technical Cyber Security Alerts
  - US-CERT (non-technical) Cyber Security Alerts
  - SANS Internet Storm Center
    - Aka DShield (Defense Shield)
  - Microsoft Security Response Center
  - Cisco Security Center

  - And many others …

Other sources of information

- Reddit r/netsec
- Twitter #infosec #cybersec
- Discord, Slack and other private and public sources
  - https://www.exploit-db.com/
  - https://vuldb.com/