

Podatności

Czym jest „podatność”

- Nieformalnie: luka, słabość lub błąd wpływający na bezpieczeństwo oprogramowania
(ang. Vulnerability)
- **Podatnością nie jest wyciek hasła z systemu. To ekspozycja**
- Sposób na wykorzystanie funkcjonalności oprogramowania w sposób który nie jest przewidziany przez twórców
- Do podatności nie należą świadomie zaimplementowane furtki/tylne wejścia/ukryte funkcjonalności (rzecz jasna po odkryciu mogą stać się sposobem na złamanie zabezpieczeń). Tu obowiązuje nazwa „tylnych drzwi”
(ang. backdoor)

Konieczność centralizacji...

- Wraz ze wzrostem ilości systemów/oprogramowania/rozwiązań, wzrosła potrzeba systematyki takich podatności
- Palącą potrzebą okazało się także jasne klasyfikowanie rodzajów błędów
- Należało także rozwiązać dylemat moralny „czy i komu zgłosić oraz kiedy”
- Każda z podatności powinna posiadać własną unikalną sygnaturę
- W przypadku przetrzymywania sygnatur w obrębie infrastruktury przedsiębiorstwa (przypadek własnego produktu), tracimy możliwość odszukania podatności wynikającego z kombinacji sprzętu i tegoż oprogramowania lub duplikujemy informację w większej ilości oddzielnych systemów

CVE

- CVE - (ang. Common Vulnerabilities and Exposures)
- Ujednolicona nazewnictwo, implementuje systematykę, ułatwia wyszukiwanie podatności
- Start projektu z inicjatywy MITRE ~1990 roku
- MITRE – organizacja non-profit, wspierana przez agencje U.S. związane z bezpieczeństwem, awiacją, obroną i wiele innych
- Poniżej centralnego rejestru CVE, znajdują się samodzielne oddziały CNA (ang. CVE Numbering Authorities)
- Otrzymują one pulę identyfikatorów dla podatności do wykorzystania przez rok
- Jeśli identyfikatory będą wykorzystane, CNA zwraca się do nadrzędnego CNA dla siebie, o uzupełnienie puli
- CNA, oznaczają podatności **wyłącznie w swoim oprogramowaniu** (IBM, Microsoft, Oracle, Goole, Gitlab...) lub pełnią funkcję dla danego kraju (nasz kraj nie ma własnego CNA)

MITRE jest także autorem frameworka ATT&CK o czym dalej

Identyfikator CVE

- Pola identyfikatora:
 - Obowiązkowe litery CVE
 - Rok rejestracji podatności
 - Sekwencyjny numer podatności
(najmniej 4 cyfrowy lub o większej długości)

CVE-2021-44228

- W przypadku pozostawienia części zakresu identyfikatora (w danym roku nie było już więcej rejestrowanych podatności przez CNA), nie są one wykorzystywane już nigdzie wykorzystywane

Podatność w CVE

- Warunki konieczne:
 - Podatność dotyczy 1 skonkretyzowanego problemu
 - Problem powinien być możliwy do naprawienia niezależnie od innych
 - Podatność posiada dowód że jest potencjalnym zagrożeniem bezpieczeństwa
 - Dotyczy jednego konkretnego produktu w określonej wersji
 - W przypadku podatności „na styku technologii”, rejestrowane są 2 CVE
 - Jest potwierdzony przez producenta/wytwórcę oprogramowania
- Lista podatności: **cve.mitre.org** lub **cve.org**
- Rejestr zawiera **publicznie rejestrowane** podatności

Dylemat moralny...

- Gradacją publiczny/prywatny, steruje CVD (ang. Coordinated Vulnerability Disclosure) które jest ewolucją z Responsible Disclosure
- Pełni rolę dobrej praktyki (a nie prawa)
- Część firm, prosi o czas przed publikacją w rejestrze na załatwienie podatności (30-90 dni). Wprowadza więc **regulowane embargo** na ujawnienie informacji
- Czasem ten czas jest wydłużany na prośbę danej firmy
- Jeśli łąta pojawia się wcześniej i jest publiczna, wyzwala to publikację w rejestrze CVE
- Opublikowana informacja o podatności bez czasu na jej załatwienie, nazywana jest **0Day**

NVD i CVSS

- Jedna z baz podatności jest NVD (ang. National Vulnerability Database)
- Pobiera dane z katalogu CVE i rozszerza wpis o remedia, szerszy opis błędu, reperkusje tegoż błędu
- Ocenia błąd według klasyfikacji CVSS (ang. Common Vulnerability Scoring System)

MITRE ATT&CK

- Autorski framework – Adversarial Tactics, Techniques & Common Knowledge
- Uporządkowana lista zachowań napastników przedstawiona w postaci taktyk i technik, przedstawiona w macierzach
- Rozszerzenie frameworka Cyber Kill Chain firmy Lockheed Martin
- Macierze ATT&CK:
 - Enterprise – systemy głównego nurtu (Windows, GNU/Linux, OsX ...)
 - Mobile – systemy mobilne
 - PRE_ATT&CK – taktyki i techniki napastnika przedsięwzięte przed i w trakcie ataku na system/rozwiązanie
- Taktyka a technika:
 - Taktyka – intencja/cel napastnika który chce go osiągnąć wykorzystując lukę
 - Technika – usystematyzowane działanie które ma doprowadzić do osiągnięcia celu

np.. Taktyka – pozyskanie dostępu do konta, Technika – brute force, ranbow table...

Macierz Enterprise

PRE-ATTACK

ENTERPRISE

RECON WEAPONIZE

DELIVER EXPLOIT INSTALL CONTROL OBJECTIVE

CyberKill Chain

PRE-ATT&CK Tactics

- ✓ Priority Definition
- ✓ Target Selection
- ✓ Information Gathering
- ✓ Weakness Identification
- ✓ Adversary OpSec
- ✓ Establish & Maintain Infrastructure
- ✓ Persona Development
- ✓ Build Capabilities
- ✓ Test Capabilities
- ✓ Stage Capabilities

ATT&CK Enterprise Tactics

- ✓ Initial Access
- ✓ Execution
- ✓ Persistence
- ✓ Privilege Escalation
- ✓ Defense Evasion
- ✓ Credential Access
- ✓ Discovery
- ✓ Lateral Movement
- ✓ Collection
- ✓ Exfiltration

Dlaczego MITRE ATT&CK ?

- Przydatność taksonomii MITRE ATT&CK
 - Integracja narzędzi – podnosi spójność obrony
 - Rozpoznanie atakujących – klasyfikacja typowych zachowań grup atakujących
 - Pro-aktywne wykrywanie zagrożeń – jeszcze przed ich wystąpieniem
 - Analiza strategiczna bezpieczeństwa cybernetycznego
 - Ujednolicenie komunikacji – wspólny słownik dobrze zdefiniowanych pojęć
 - Decyzja zakupowa/wdrożeniowa/konfiguracyjna – maksymalizacja ROSI (ang. Return on Security Investment)

Kilka źródeł

- ATT&CK Navigator – mapowanie taktyk i technik
<https://mitre-attack.github.io/attack-navigator/>
- Anomali Cyber Watch Ten – cotygodniowy bezpłatny raport raportujący zmiany w zakresie bezpieczeństwa w danym tygodniu
<https://www.anomali.com/resources/anomali-cyber-watch>
- MITRA Caldera – narzędzie symulacji przeciwników
<https://caldera.mitre.org/>
- Endgame RedTeam Automation – testowanie złośliwego zachowania
<https://github.com/endgameinc/RTA>
- ATT&CK Tableau Table – arkusze do analizy
<https://github.com/Cyb3rPandaH/Tableau-ATTCK>
- Blog MITRE ATT&CK
<https://medium.com/mitre-attack>