Információs rendszerek biztonságtechnikája

Sebezhetőségek

Vakulya Gergely

A sebezhetőségek

- A sebezhetőség bizonyos rendszerek, szoftverek gyengesége, amit egy támadó a saját céljaira, illetve károkozásra tud kihasználni.
- A sebezhetőséget kihasználó szoftver az exploit.
- A következők időbeli alakulása lényegében tetszőlegesen alakulhat:
  - A sebezhetőségek fennállásának időintervalluma
  - Azok felfedezése
  - A javítások elkészítése (a sebezhetőség befoltozása)
  - A sebezhető rendszerek tényleges javítása
  - A sebezhetőség nyilvánosságra hozása
  - A sebezhetőség ismert, vagy feltételezett kihasználása

A CVE adatbázis

- CVE: Common Vulnerabilities and Exposures
- Nyilvános sérülékenység-adatbázis.
- A publikált sérülékenységek egy CVE számot kapnak, amiről egyértelműen be lehet őket azonosítani (emellett lehet fantázianevük is).
- Legfontosabb információk:
  - Milyen szoftvert (vagy egyéb rendszert érint)
  - Milyen verziókat érint
  - Rögzítés dátuma
  - Leírás (működési mechanizmus)
  - Referenciák (például az egyes szállítók információihoz)
- Több gyűjtőoldal:
  - https://cve.mitre.org
  - https://www.cvedetails.com
  - https://www.cve.org/
  - https://nvd.nist.gov

A sebezhetőségek fő típusai

- Kódfuttatás (**code execution**): A támadó (esetenként tetszőleges) kódot képes futtatni a sebezhető rendszeren.
- Védelem, vagy ellenőrzés megkerülése (**bypass**): A támadó valamilyen ellenőrzés kihagyására képes a sebezhető rendszert késztetni.
- Privilégiumszint emelés (**privilege escalation**): A támadó egy számára nem biztosított privilégiumhoz (például root joghoz) jut.
- Szolgáltatásmegtagadás (**denial of service, DoS**): A támadó a rendszer szolgáltatásait leállítja, lelassítja, vagy azokat valamilyen módon akadályozza.
- Adatszivárgás (**information leak**): A támadó számára nem nyilvános adatokhoz jut.

Támadási mechanizmusok

- Puffertúlcsordulásos támadás (buffer overflow, stack buffer overflow)
- SQL-injektálás (SQL injection, SQLi)
- Cross-side scripting, XSS
- Kéréshamisítás (Cross-site request forgery, CSRF vagy XSRF)
- Versenyhelyzet (Race condition)
- Sidechannel attack
- Memory corruption
- Bemenet ellenőrzés (Input validation)
- Kriptográfiai támadások

Ezek kombinációi is gyakoriak.

CVE-2019-18634, sudo pwfeedback exploit (Linux és egyéb rendszerek)

- A sudo 1.7.1 (2009-04-11) és 1.8.26 (2018-11-13) verziói között.
- A `sudo` parancs a jelszó bekérésekor nem ad kimenetet.
- Azonban beállíthatjuk, hogy a jelszó begépelése közben csillagok jelenjenek meg.
- Ha ez a beállítás fennáll, megfelelően összeállított bemenet beírásával a támadó root jogosultsághoz juthat.
- Típus: Helyi privilégiumszint növelés (local root).
- Mechanizmus: Stack buffer overflow.
- Megjegyzés: A ‘sudo‘ root joggal fut.

CVE-2016-5195, Dirty COW (Linux)

- Linux kernel, 2.x-4.x, a 4.8.3 előtt.
- COW jelentése: Copy On Write
- Versenyhelyzet (race condition) alapú sebezhetőség.
- A kihasználásával a támadó egy olyan, a root tulajdonában levő fájlt tud írni, amire csak olvasási joga van.
  - Átírhat konfigurációs fájlokat, például jogosultságokat adva magának.
  - Backdoort helyezhet el valamelyik setuid root-os programban.

A Dirty COW működése

- Unix alatt „minden file”. A `/proc` alatt például virtuális fájlok vannak. A `/proc/self/mem` az aktuális folyamat memóriájának leképezése.
- `mmap()` függvény: Egy fájlt a memóriára képez le.
- Saját COW másolatot is készíthetünk egy fájlról.
- Copy on write: Csak akkor másolja le ténylegesen, ha módosítjuk.
- Race condition: Két eseménynak egymáshoz képest speciálisan időzítve kell lefutnia a hibához.
- Két thread-et futtatunk:
  - Az egyikben az `madvice()` függvénnyel azt mondjuk a kernelnek, hogy az adott területet nem fogjuk a közeljövőben használni.
  - A másikban a saját memóriát leképező `/proc/self/mem` azon részére írunk, ahova a támadott fájlt map-eltük.
- Nagyon sok próbálkozás után egy bizonyos ponton a kernel „elrontja” az írás és a másolás sorrendjét és felülíródik a megnyitt fájl.

CVE-2017-5754, Meltdown (operációs rendszertől független)

CVE-2017-0199, Office arbitrary code execution

CVE-2017-0144, Eternal Blue

Slow loris (CVE-2007-6750 és sok egyéb)

CVE-2020-0796 aka CoronaBlue aka SMBGhost