♀ Øvelse 50 – (Gruppeøvelse) Undersøgelse af CVE'er

Formål

Formålet med denne øvelse er at give jer praktisk erfaring med at undersøge **kendte sårbarheder (CVE'er)** ved hjælp af forskellige online databaser. I skal forstå den bagvedliggende svaghed, hvordan den udnyttes, samt vurdere alvorligheden via **CVSS-score**. Øvelsen giver jer indblik i, hvordan CVE'er dokumenteres og bruges i sikkerhedsvurdering og -monitorering.

Baggrund

CVE står for *Common Vulnerabilities and Exposures* og er en unik identifikator for kendte sårbarheder. CVE'er anvendes i stort set alle sikkerhedsværktøjer og bruges i praksis til risikovurdering, patch management og trusselsanalyse.

CVE'er findes i forskellige databaser – herunder Mitre, CVE Details og Tenable – som hver især kan give overblik over sårbarhedens tekniske karakter, påvirkede systemer, exploit-muligheder og CVSS-score (Common Vulnerability Scoring System).

Instruktioner

I jeres gruppe skal I undersøge følgende CVE'er:

- CVE-2023-32269
- CVE-2023-31436
- CVE-2014-0160
- CVE-2022-47509
- CVE-2021-44228
- CVE-2022-26903

For hver sårbarhed skal I finde følgende informationer:

- En kort og præcis konceptuel forklaring på, hvad sårbarheden går ud på
- Hvilken type sårbarhed det er (f.eks. RCE, DoS, privilege escalation, info leak)

- Hvilke systemer eller komponenter der er berørt
- Den tilknyttede **CVSS-score**, og hvad den fortæller om alvorligheden

> I må gerne fordele sårbarhederne i gruppen og fremlægge resultaterne for hinanden efterfølgende.

Nyttige links

- Mitre CVE-database
- CVE Details
- Tenable CVE Search

Refleksionsspørgsmål

- Hvordan kan CVE'er bruges i praksis til at prioritere sikkerhedsarbejde?
- Hvad er forskellen på en høj CVSS-score og reel trusselsaktivitet?
- Hvilke sårbarheder fandt I mest alvorlige – og hvorfor?
- Hvordan kunne man bruge Wazuh eller andre værktøjer til at detektere eller håndtere disse sårbarheder?

Last update: 2026-03-20 13:58:28