cesnet

Zranitelnosti jak je neznáte

Radko Krkoš

CESNET, z.s.p.o.

07.02.2023

Seminář bezpečnosti sítí a služeb 2023, Praha

Čo je zraniteľnosť?

- **Zraniteľnosť:**
  - slabé miesto aktíva alebo slabé miesto bezpečnostného opatrenia, ktoré môže byť zneužité jednou či viacerými hrozbami (VoKB),
  - vlastnosť aktíva, ktorá ho činí citlivým na poškodenie alebo zničenie.
- **Hrozba:**
  - akýkoľvek fenomén, ktorý má potenciálnu schopnosť poškodiť aktívum (adaptované z Bezpečnostnej stratégie ČR).

Ako popísať konkrétnu zraniteľnosť?

- **CVE:**
  - MANN, David E. a Steven M. CHRISTEY. Towards a Common Enumeration of Vulnerabilities. 2nd Workshop on Research with Security Vulnerability Databases. Purdue University, West Lafayette, Indiana, USA, January 8, 1999, 1999(January 21-22), 13s.

  1) „… define vulnerabilities with only the necessary and sufficient **attributes that are common to all vulnerabilities**,
  2) ensuring that these attributes **do not rely on any evolving representation** and
  3) can be commonly **agreed to by the** majority of the **security community**.“

  - Common Vulnerability Enumeration -> Common Vulnerabilities & Exposures.

Implementácia

- CVE-yyyy-nnnn,
- 195103 zraniteľností v katalógu (ku 06.02.2023),
- September 1999, zadané spätne – 01.01.1999 (príp. staršie),
- CVE-1999-0497 - Anonymous FTP is enabled,
- CVE-1999-0523 - ICMP echo (ping) is allowed from arbitrary hosts,
- CVE-1999-0613, CVE-1999-0624, CVE-1999-0625, CVE-1999-0629, CVE-1999-0635, CVE-1999-0637, CVE-1999-0638, CVE-1999-0639, CVE-1999-0641, …
  - The XXX service is running.
  - chargen, echo, systat, UUCP, identd, rstat, RPC portmapper, daytime...

CVE-1999-0001

- ip_input.c in BSD-derived TCP/IP implementations allows **remote attackers** to cause a **denial of service** (crash or hang) via **crafted packets**,
- Opravená napr. v OpenBSD 2.4, vydanom 1. decembra 1998, patch z 13. novembra 1998,
- CVE-2019-11477: TCP SACK PANIC,
- CVE-2022-41674, CVE-2022-42719 – CVE-2022-42722: Linux 5.1 – 6.0.2, mac80211 – DoS, RCE.

CVE-2007-5908

- **Buffer overflow** in the (1) sysfs_show_available_clocksources and (2) sysfs_show_current_clocksources functions in Linux kernel 2.6.23 and earlier might allow local users to cause a **denial of service** or **execute arbitrary code** via **crafted clock source names**.
- NOTE: follow-on analysis by Linux developers states that "**There is no way** for unprivileged users (or really even the root user) **to add new clocksources**."
- **REJECT**.

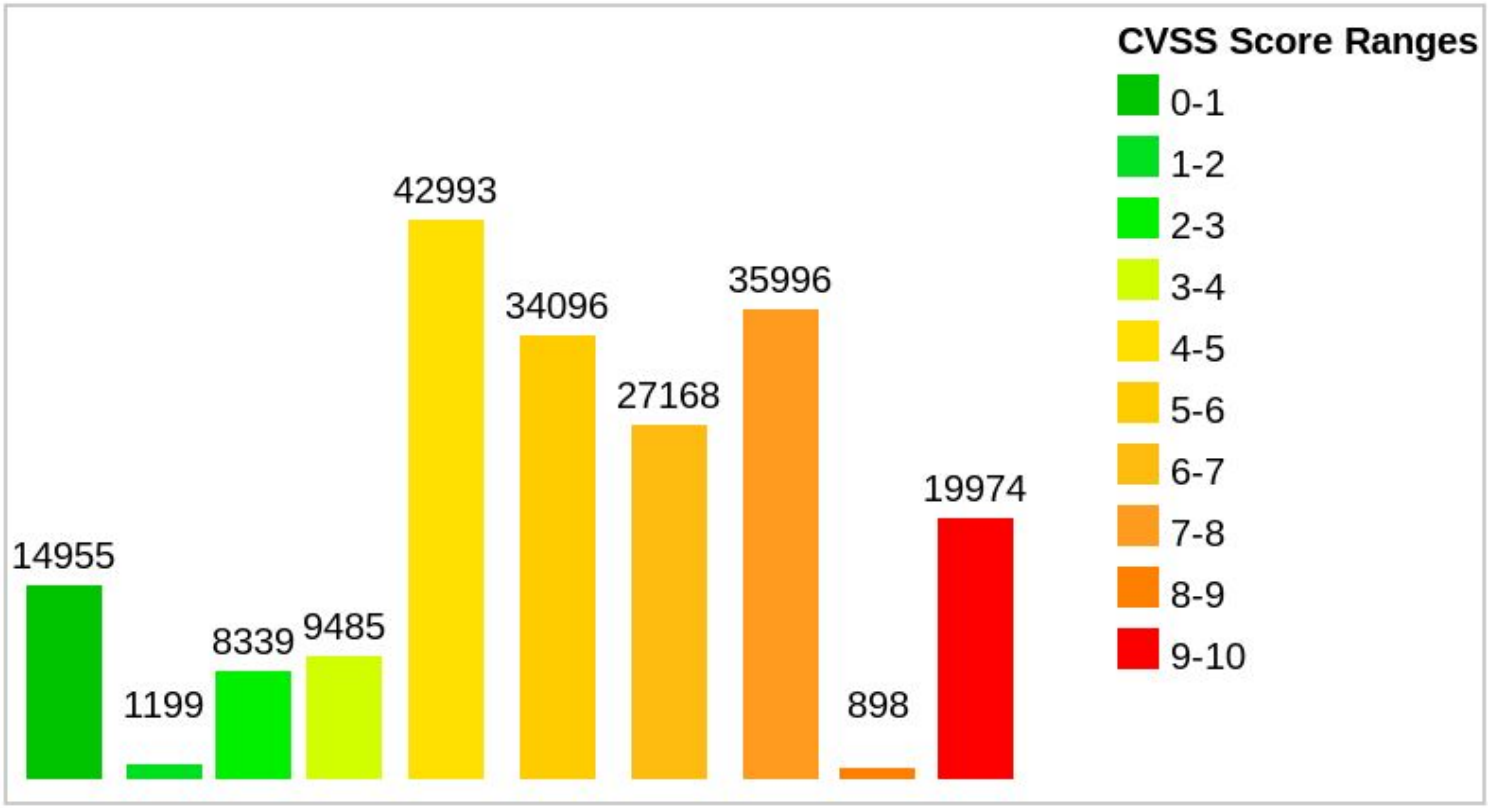
Ako hodnotiť zraniteľnosť?

- CVSS – Common Vulnerability Scoring System,
- Aktuálna verzia 3.1, Forum of Incident Response and Security Teams,
- Hodnota 0,0 – 10,0 priamo úmerná závažnosti zraniteľnosti,
  - Žiadna: 0; Nízka 0,1-3,9; Stredná 4-6,9; Vysoká 7-8,9; Kritická 9-10;
- Metriky:
  - Základné – univerzálne,
  - Temporálne – stav exploitu, dostupnosť opravy,
  - Environmentálne – unikátne vzhľadom ku prostrediu,

Základné metriky CVSS

- **Attack Vector (AV):**
  - Network (N), Adjacent (A), Local (L), Physical (P)
- **Attack Complexity (AC):**
  - Low (L), High (H)
- **Privileges Required (PR):**
  - None (N), Low (L), High (H)
- **User Interaction (UI):**
  - None (N), Required (R)
- **Scope (S):**
  - Unchanged (U), Changed (C)
- **Confidentiality (C), Integrity (I), Availability (A):**
  - None (N), Low (L), High (H)

Rozloženie závažnosti podľa CVSS



Zdroj: www.cvedetails.com

Čo ďalej?

- Monitorujte zraniteľnosti,
- Spolupracujte s nami:
  - Staňte sa členom alebo členkou CESNET SOC:
    - www.cesnet.cz -> „O nás“ -> Člen/ka Security Operation Center CESNET,
  - Podelíme sa o prácu,
- Odoberajte naše výstupy:
  - mailto:csirt-forum-subscribe@cesnet.cz, alebo sluzby@cesnet.cz.

Dobrú chuť!

- Otázky a diskusie v rámci prestávky.