Amenințările informaționale sunt evenimente sau acțiuni care au potențialul de a compromite securitatea informației. Acestea pot include:

1. **Atacuri asupra serviciilor web și cloud**: Serviciile web și cloud devin din ce în ce mai importante în mediul IT modern, iar atacatorii pot viza aceste servicii pentru a obține acces neautorizat la date sau pentru a perturba funcționarea acestora.
    - "Apache HTTP Server 2.4.50 - Remote Code Execution (RCE)", indică o problemă de securitate care afectează versiunea 2.4.50 a serverului web Apache HTTP. Această vulnerabilitate este clasificată ca fiind de tip "Remote Code Execution" (RCE), ceea ce înseamnă că un atacator poate executa cod de la distanță pe serverul afectat. https://www.exploit-db.com/exploits/50512
    - Vulnerabilitatea CVE-2021-41773 în serverul web Apache HTTP Server 2.4.49 și 2.4.50 permite unui atacator să acceseze fișiere din afara directorului rădăcină al serverului. Această expunere poate dezvălui informații sensibile despre configurarea serverului și alte date importante, ceea ce ar putea fi utilizat pentru a compromite securitatea serverului și a sistemelor asociate. Este crucial ca administratorii să aplice rapid actualizările și remedierile necesare pentru a proteja serverele lor împotriva acestei vulnerabilități. https://www.exploit-db.com/exploits/51546
2. **Atacuri asupra infrastructurii fizice sau a dispozitivelor IoT**
    - Amcrest Cameras 2.520.AC00.18.R - Unauthenticated Audio Streaming. Această vulnerabilitate a afectat

dispozitivele Cisco Small Business SPA514G IP Phone și a permis atacatorilor să execute cod arbitrar prin intermediul unei conexiuni de rețea. https://www.exploit-db.com/exploits/47188

3. **Atacuri de tip DDoS**
    - Apple macOS/iOS - Multiple Kernel Use-After-Frees due to Incorrect IOKit Object Lifetime Management in IOTimeSyncClockManagerUserClient. Această vulnerabilitate este legată de gestionarea necorespunzătoare a obiectelor IOKit în cadrul modulului IOTimeSyncClockManagerUserClient. Exploatarea acestei vulnerabilități ar putea permite unui atacator local să execute cod de la distanță cu privilegii ridicate pe dispozitivul afectat, ceea ce ar putea duce la preluarea controlului asupra sistemului sau la compromiterea datelor stocate pe dispozitiv. Pentru a remedia această vulnerabilitate, Apple a lansat actualizări de securitate pentru macOS și iOS, iar utilizatorii sunt încurajați să-și actualizeze dispozitivele la cele mai recente versiuni de software pentru a se proteja împotriva exploatării acestei vulnerabilități. https://www.exploit-db.com/exploits/43326
    - PHP 5.3.1 - 'session_save_path() Safe_mode()' Restriction Bypass Exploiot. Vulnerabilitatea menționată este legată de PHP 5.3.1 și este asociată cu o circumstanță în care funcția 'session_save_path()' este capabilă să ocolească restricțiile impuse de 'safe_mode()'. Acest lucru poate permite atacatorilor să efectueze acțiuni care altfel ar fi interzise sau limitate în cadrul mediului PHP. Practic, 'safe_mode()' este o caracteristică în versiunile mai vechi

ale PHP care încearcă să ofere un anumit nivel de protecție prin restricționarea accesului scripturilor PHP la anumite resurse de sistem. Cu toate acestea, există circumstanțe în care aceste restricții pot fi evitate sau ocolite, permițând unor actori rău intenționați să efectueze acțiuni nedorite sau periculoase. https://www.exploit-db.com/exploits/33625