Sårbarheter och attacker

Del av kursen ETE352 Cybersäkerhet – grunder och medvetenhet som ges vid Linköpings universitet

Mikael Asplund

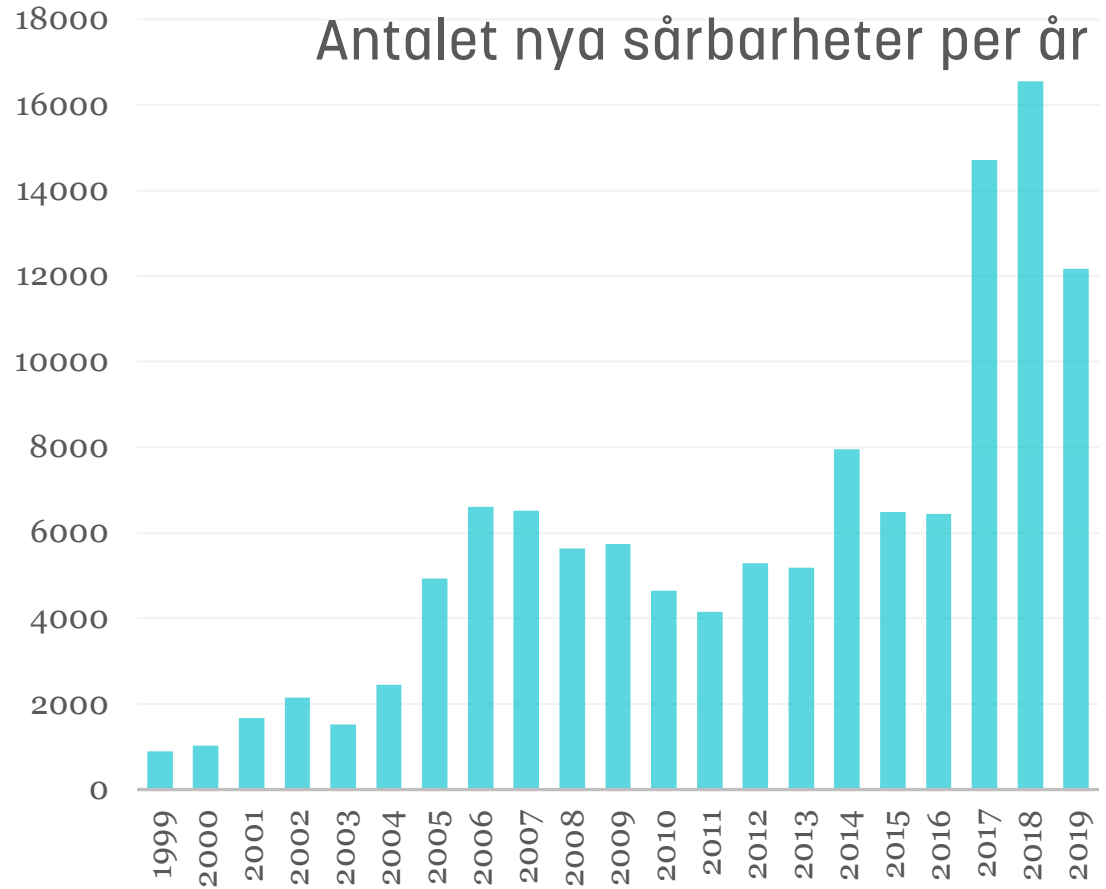
LINKÖPINGS UNIVERSITET

Hot

- Engelska: threat
- Samlande begrepp för händelser eller objekt som kan orsaka skada för ett system
- Inkluderar både avsiktliga och oavsiktliga händelser
  - Avsiktliga i form av attacker
  - Oavsiktliga i form av felkälla, felyttring, och haveri (fault, error, failure)

Sårbarheter

- Engelska: vulnerability
- En svaghet i systemet som *möjliggör* attacker
- Sårbarheter kan finnas i
  - Systemdesign
  - Mjukvara
  - Hårdvara
  - Organisation
  - Policy och rutiner



Vulnerability Details : CVE-2021-42071

In Visual Tools DVR VX16 4.2.28.0, an unauthenticated attacker can achieve remote command execution via shell metacharacters in the cgi-bin/slogin/login.py User-Agent HTTP header.

Publish Date : 2021-10-07 Last Update Date : 2021-10-15

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	**10.0**
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	78

– Products Affected By CVE-2021-42071

#	Product Type	Vendor	Product	Version	Update	Edition	Language

No vulnerable product found. If the vulnerability is created recently it may take a few days to gather vulnerable products list and other information like cvss scores. Please check again in a few days.

– References For CVE-2021-42071

https://www.swascan.com/security-advisory-visual-tools-dvr-cve-2021-42071/

https://visual-tools.com/

https://www.exploit-db.com/exploits/50098

Exploit

- Mjukvara som utnjyttjar en sårbarhet
- “Weaponizing a vulnerability”
- Ramverk för exploits
  - Tex Metasploit
  - Dual use
  - Lätt att skapa varianter

Attack

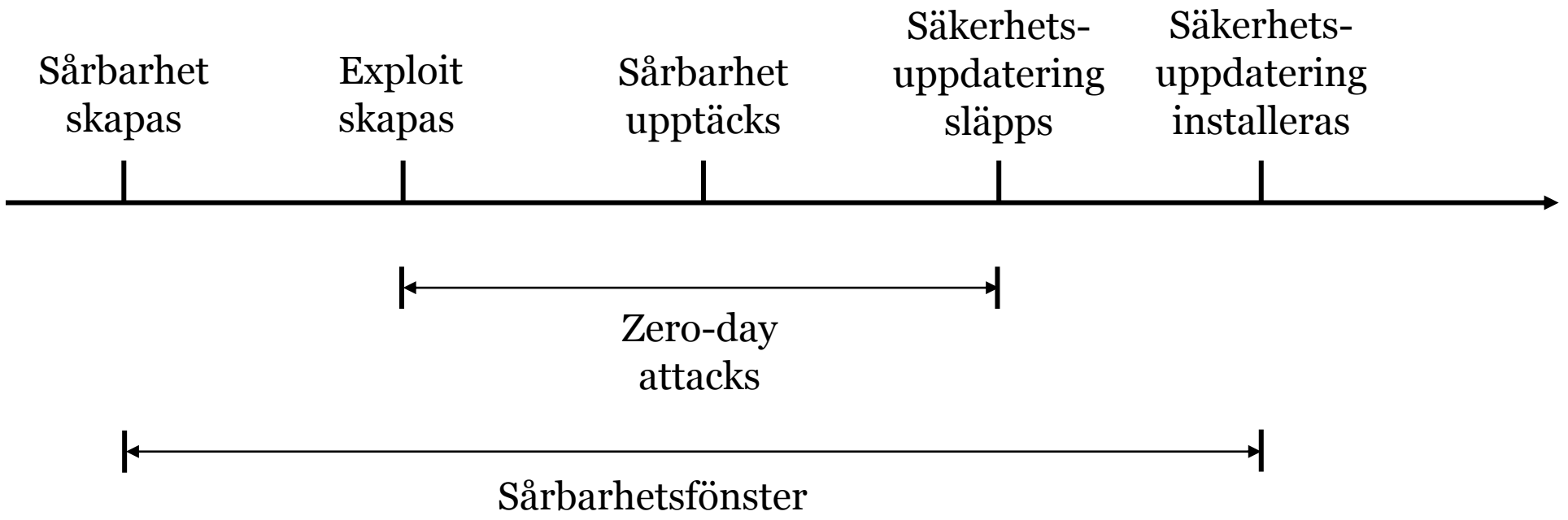
- Även cyberattack
- En medveten handling som hotar skyddsvärda egenskaper för ett system
- Utförs av en hotagent (threat agent)

Några vanliga typer av attacker

- Social engineering/Phishing
- Remote code execution
- Privilege escalation
- Denial-of-Service (DoS)
- Man-in-the-middle (MitM)
- Spoofing
- Spyware/ransomware
- Password attacks

Sårbarhetsfönster

Vulnerability Window



https://cybersakerhet-grund.ida.liu.se

LINKÖPINGS UNIVERSITET