CVE-2020-13519

- A privilege escalation vulnerability aftecintg the device driver
- Version 4.8.0 affected
- NZXT CAM monitoring software
- 8.8 CVSS SCORE

CVE-2022-31144

Redis server remote code execution. A specially crafted `XAUTOCLAIM` command on a stream key in a specific state may result in RCE

versions prior to 7.0.4

8.8 CVSS SCORE

Exploit Catalogue

Your Path for a Successfull CyberSec Business

CVE-2024-7400

A vulnerability which allowes an attacker to misuse ESET's file operations during the removal of a detected file on the Windows operating system and allows a low-privileged attacker tobtain NT AUTHORITY\SYSTEM privileges!

CVE-2024-25648

- A use-after-free vulnerability which allows privillege escalation
- Version 2024.1.0.23997 affected
- Foxit Reader software
- 8.8 CVSS SCORE

CVE-2022-23270

A use-after-free vulnerability which allows privillege escalation due to a Double Free that occurs as the result of a race condition.

Windows Point-to-Point Tunneling Protocol

Windows 10 Version 1901-21h2

8.1 cvss score

CVE-2022-26937

A stack buffer overflow vulnerability in nfssvr driver. The exploit for this particular vulnerability will be a full chain with another vuln. Side channel info leak

Windows Network File System

Windows Server, version 20H2

9.8 cvss score

CVE-2022-21972

A use-after-free vulnerability which allows privillege escalation due to a Double Free that occurs as the result of a race condition.

Windows Point-to-Point Tunneling Protocol

Windows Server, version 20H2

8.1 cvss score

CVE-2020-35533

An out-of-bounds read vulnerability which will be used as part of a vulnerability chain in order to obtain remote code exec when parsing images in linux

Libraw of ImgeaMagick 7.0.10

Ubuntu 18.04

5.5 cvss score