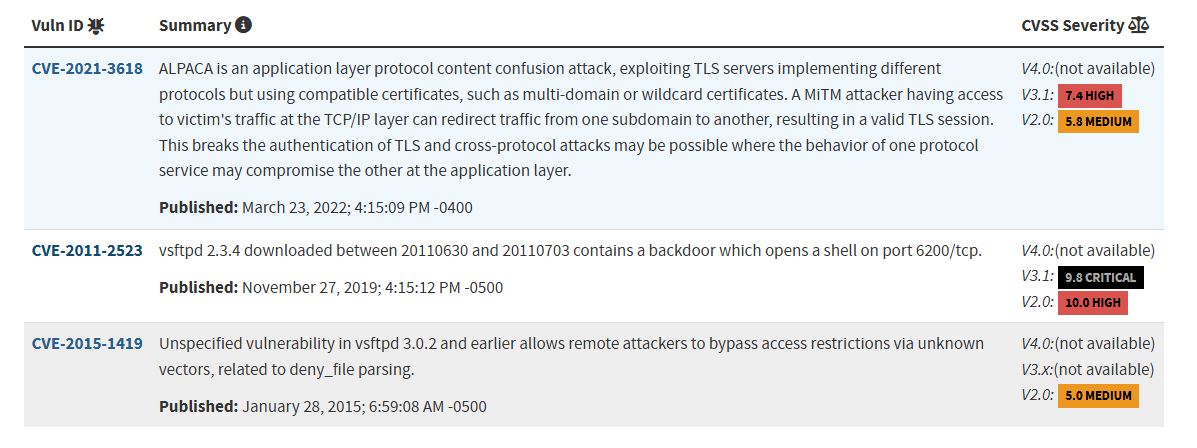
# MAPPING VULNERABILITIES - EXPLOIT IS AVAILABLE OR NOT

Checking for available Exploits on web, for versions, open ports, backdoor where we can enter to a particular network or a host. Taking resources from NVD, where we can get a CVE number to deep dive into a particular exploit. CVE means Common vulnerabilities & exposures, by using CVE we can identify weather the exploit is still accessible or closed.

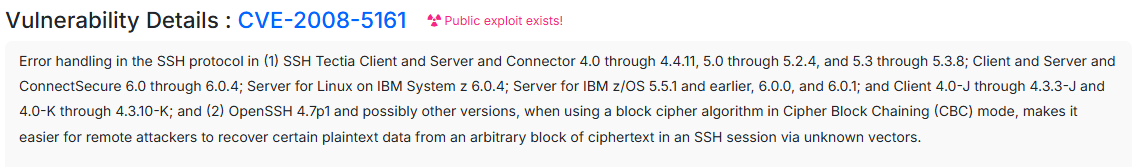
**FTP server version : vsFTPd 2.3.4**

CVE-2011-2523, CVE-2015-1419, CVE-2021-3618 details : We can’t exploit it right now as it was closed.

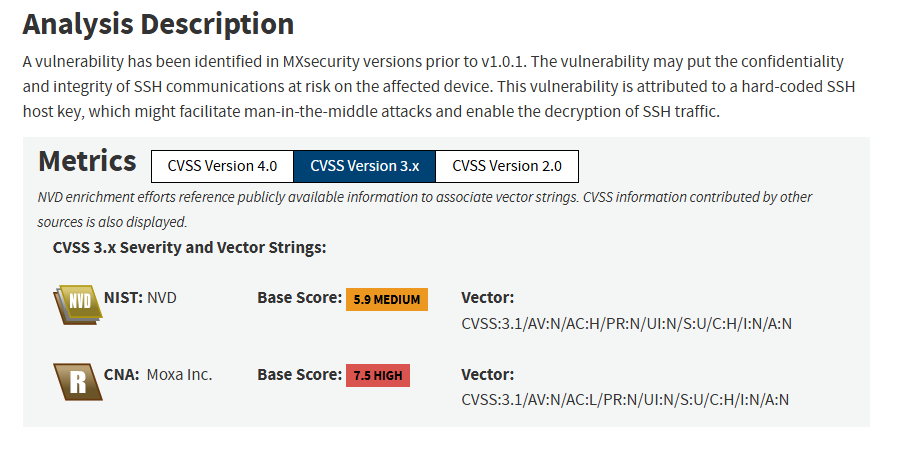


**Open SSH 4.7p1 : Security Vulnerabilities**

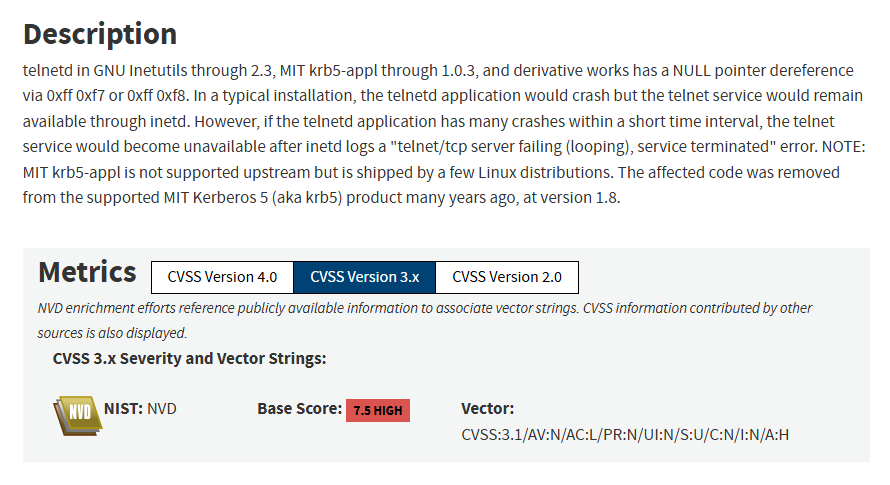
CVE-2008-5161 : We can’t exploit it right now as it was closed.



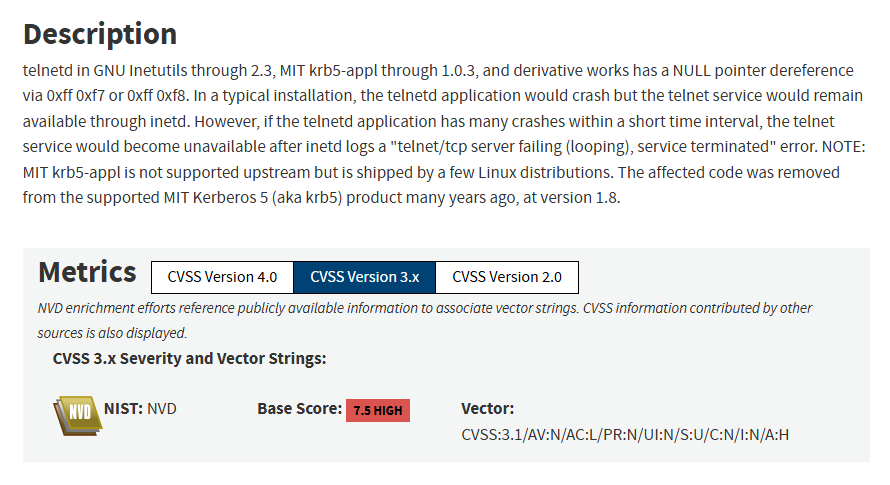
**Host Key Vulnerability details :** CVE-2023-39982

****

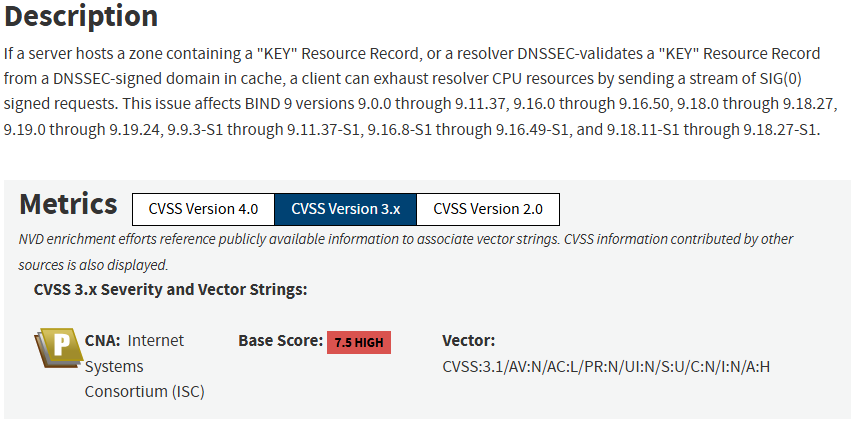
## **Linux telnetd port 23 Vulnerablities :** CVE-2022-39028



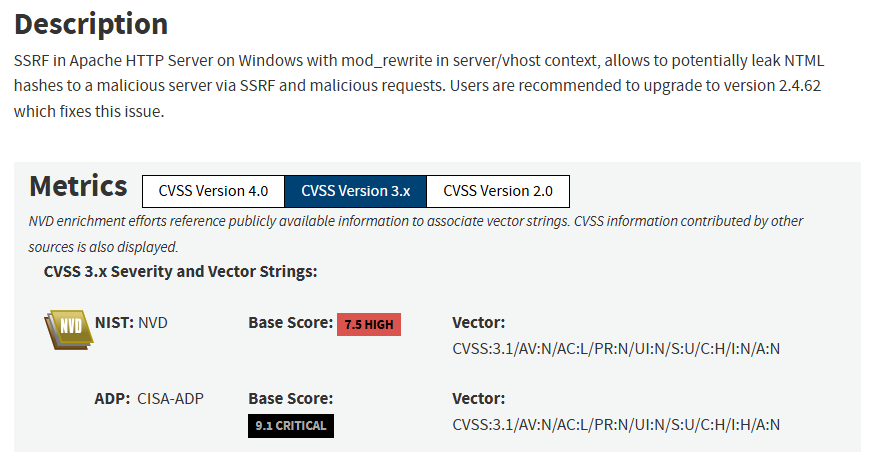
# **SMTP server in Postfix :** [CVE-2011-1720](https://www.cvedetails.com/cve/CVE-2011-1720/" \o "CVE-2011-1720 security vulnerability details)



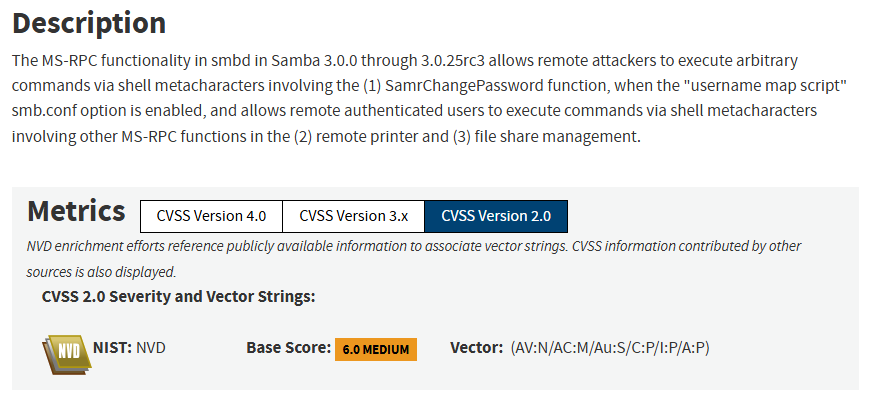
**DNS bind.version: 9.4.2 :** CVE-2024-1975



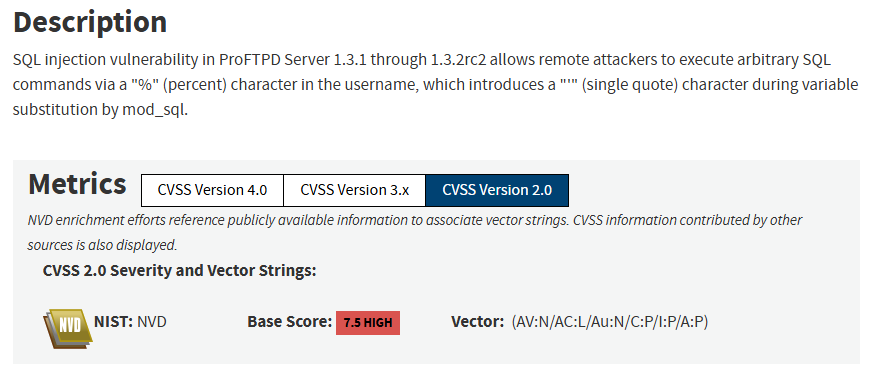
**Apache http 2.2.8 :** CVE-2024-40898



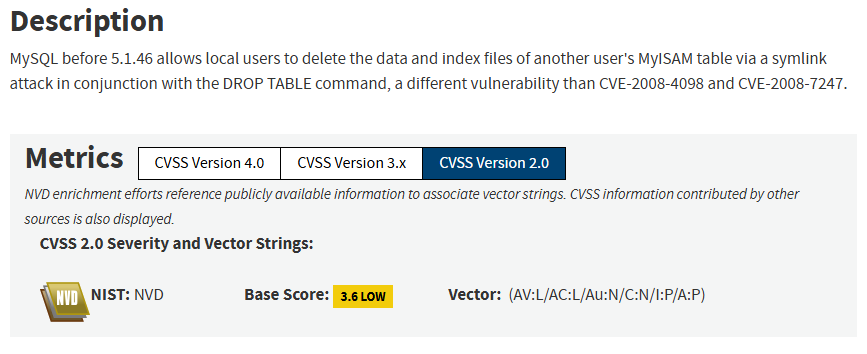
**Samba smbd 3.0.20 :** CVE-2007-2447



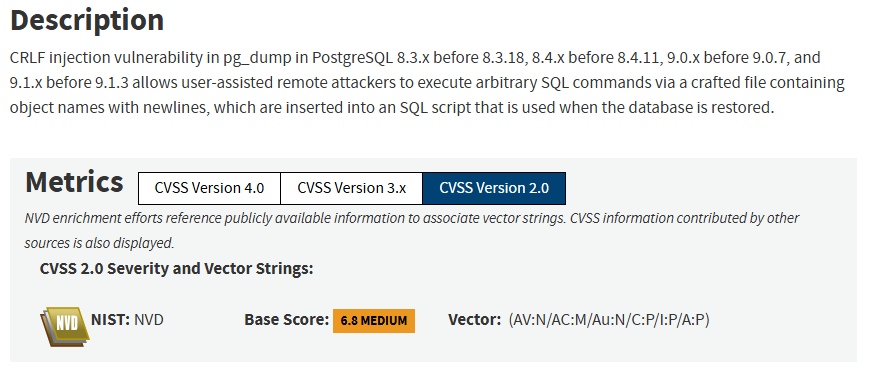
**ProFTPD 1.3.1 :** CVE-2009-0542



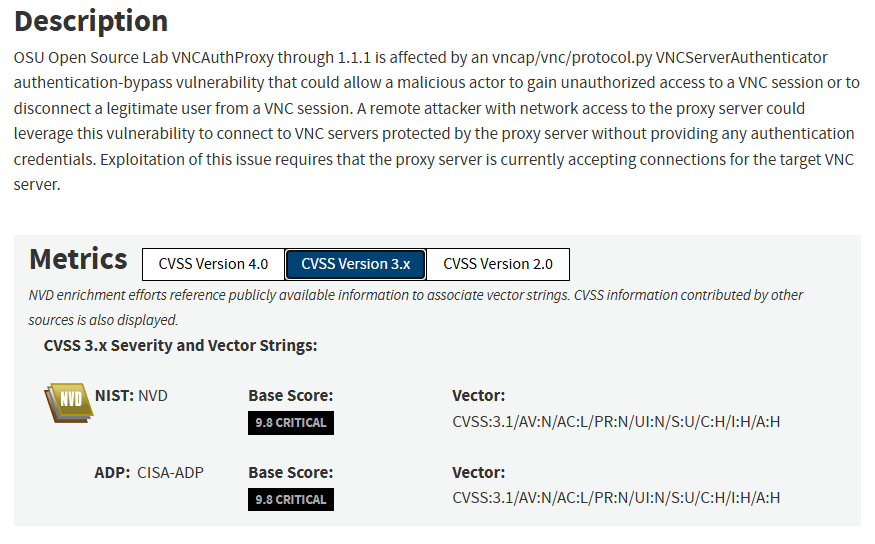
**MySQL 5.0.51 :** CVE-2010-1626



**PostgreSQL DB 8.3.0 - 8.3.7 :** CVE-2012-0868



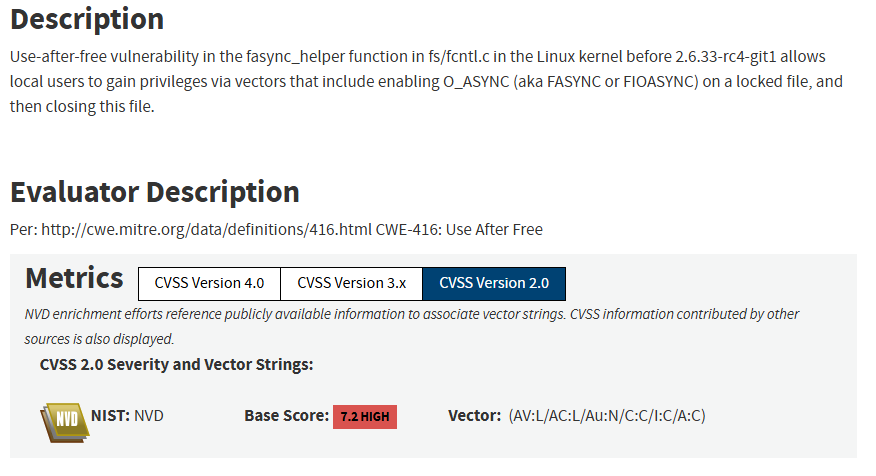
## VNC (protocol 3.3) : CVE-2022-36436



**Apache Tomcat/5.5 :** CVE-2008-0128



**Linux 2.6.9 - 2.6.33 :** CVE-2009-4141



**Summary :** All the above vulnerabilities are few of them exploited in the past are closed and got fixed. Using the CVE number we have identified weather the exploit is still available or not. We also understood impact of the attack on the services, by see the cvss.