Vulnerability Assessment

10/31/2021, 05:30:30

IP Address:35.239.85.118

Ports scanned: 0-80

Port scan

Port 22 open

Port 80 open

Searchsploit results

-------------------------------- Exploit Title | Path

-------------------------------- Debian   8[01;31m 8[KOpenSSH 8[m 8[K - (Authenticated) Remote SELinux Privilege Escalation | linux/remote/6094.txt Dropbear /
   8[01;31m 8[KOpenSSH 8[m 8[K Server - 'MAX_UNAUTH_CLIENTS' Denial of Service | multiple/dos/1572.pl FreeBSD   8[01;31m 8[KOpenSSH 8[m 8[K 3.5p1 - Remote Command Execution | freebsd/remote/17462.txt glibc-2.2 /
   8[01;31m 8[Kopenssh 8[m 8[K-2.3.0p1 / glibc 2.1.9x - File Read | linux/local/ 258.sh Novell Netware 6.5 - 8[01;31m 8[KOpenSSH 8[m 8[K Remote Stack Overflow | novell/dos/14866.txt   8[01;31m 8[KOpenSSH 8[m 8[K 1.2 - '.scp' File Create/Overwrite | linux/remote/20253.sh   8[01;31m 8[KOpenSSH 8[m 8[K 2.3 < 7.7 - Username Enumeration | linux/remote/45233.py
   8[01;31m 8[KOpenSSH 8[m 8[K 2.3 < 7.7 - Username Enumeration (PoC) | linux/remote/45210.py   8[01;31m 8[KOpenSSH 8[m 8[K 2.x/3.0.1/3.0.2 - Channel Code Off-by-One | unix/remote/21314.txt
   8[01;31m 8[KOpenSSH 8[m 8[K 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow | linux/remote/21402.txt   8[01;31m 8[KOpenSSH 8[m 8[K 3.x - Challenge-Response Buffer Overflow (1) | unix/remote/21578.txt
   8[01;31m 8[KOpenSSH 8[m 8[K 3.x - Challenge-Response Buffer Overflow (2) | unix/remote/21579.txt   8[01;31m 8[KOpenSSH 8[m 8[K 4.3 p1 - Duplicated Block Remote Denial of Service | multiple/dos/2444.sh
   8[01;31m 8[KOpenSSH 8[m 8[K 6.8 < 6.9 - 'PTY' Local Privilege Escalation | linux/local/41173.c   8[01;31m 8[KOpenSSH 8[m 8[K 7.2 - Denial of Service | linux/dos/40888.py   8[01;31m 8[KOpenSSH 8[m 8[K 7.2p1 - (Authenticated) xauth Command Injection | multiple/remote/39569.py
   8[01;31m 8[KOpenSSH 8[m 8[K 7.2p2 - Username Enumeration | linux/remote/ 40136.py   8[01;31m 8[KOpenSSH 8[m 8[K < 6.6 SFTP (x64) - Command Execution | linux_x86-64/remote/45000.c   8[01;31m 8[KOpenSSH 8[m 8[K < 6.6 SFTP - Command Execution | linux/remote/45001.py
   8[01;31m 8[KOpenSSH 8[m 8[K < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
   8[01;31m 8[KOpenSSH 8[m 8[K < 7.4 - agent Protocol Arbitrary Library Loading | linux/remote/40963.txt   8[01;31m 8[KOpenSSH 8[m 8[K < 7.7 - User Enumeration (2) | linux/remote/45939.py   8[01;31m 8[KOpenSSH 8[m 8[K SCP Client - Write Arbitrary Files | multiple/remote/46516.py
   8[01;31m 8[KOpenSSH 8[m 8[K/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident | linux/remote/26.sh   8[01;31m 8[KOpenSSH 8[m 8[K/PAM 3.6.1p1 - Remote Users Discovery Tool | linux/remote/25.c   8[01;31m 8[KOpenSSH 8[m 8[Kd 7.2p2 - Username Enumeration | linux/remote/40113.txt Portable

8[01;31m 8[KOpenSSH 8[m 8[K 3.6.1p-PAM/4.1-SuSE - Timing Attack | multiple/remote/3303.sh

----

------------------------------- Shellcodes: No Results