



192.168.43.240

[FULLSCAN]

2022-07-31 15:57

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 (protocol 2.0; HPN-SSH patch 14v4)

| vulners:

| cpe:/a:openbsd:openssh:7.2p2:

| PACKETSTORM:140070 7.8 <https://vulners.com/packetstorm/PACKETSTORM:140070> *EXPLOIT*

| EDB-ID:40888 7.8 <https://vulners.com/exploitdb/EDB-ID:40888> *EXPLOIT*

| CVE-2016-8858 7.8 <https://vulners.com/cve/CVE-2016-8858>

| CVE-2016-6515 7.8 <https://vulners.com/cve/CVE-2016-6515>

| 1337DAY-ID-26494 7.8 <https://vulners.com/zdt/1337DAY-ID-26494> *EXPLOIT*

| SSV:92579 7.5 <https://vulners.com/seebug/SSV:92579> *EXPLOIT*

| CVE-2016-10009 7.5 <https://vulners.com/cve/CVE-2016-10009>

| 1337DAY-ID-26576 7.5 <https://vulners.com/zdt/1337DAY-ID-26576> *EXPLOIT*

| SSV:92582 7.2 <https://vulners.com/seebug/SSV:92582> *EXPLOIT*

| CVE-2016-10012 7.2 <https://vulners.com/cve/CVE-2016-10012>

| CVE-2015-8325 7.2 <https://vulners.com/cve/CVE-2015-8325>

| SSV:92580 6.9 <https://vulners.com/seebug/SSV:92580> *EXPLOIT*

| CVE-2016-10010 6.9 <https://vulners.com/cve/CVE-2016-10010>

| 1337DAY-ID-26577 6.9 <https://vulners.com/zdt/1337DAY-ID-26577> *EXPLOIT*

| EDB-ID:46516 5.8 <https://vulners.com/exploitdb/EDB-ID:46516> *EXPLOIT*

| EDB-ID:46193 5.8 <https://vulners.com/exploitdb/EDB-ID:46193> *EXPLOIT*

| CVE-2019-6111 5.8 <https://vulners.com/cve/CVE-2019-6111>

| 1337DAY-ID-32328 5.8 <https://vulners.com/zdt/1337DAY-ID-32328> *EXPLOIT*

| 1337DAY-ID-32009 5.8 <https://vulners.com/zdt/1337DAY-ID-32009> *EXPLOIT*

| SSV:91041 5.5 <https://vulners.com/seebug/SSV:91041> *EXPLOIT*

| PACKETSTORM:140019 5.5 <https://vulners.com/packetstorm/PACKETSTORM:140019> *EXPLOIT*

| PACKETSTORM:136234 5.5 <https://vulners.com/packetstorm/PACKETSTORM:136234> *EXPLOIT*

| EDB-ID:40858 5.5 <https://vulners.com/exploitdb/EDB-ID:40858> *EXPLOIT*

| EDB-ID:40119 5.5 <https://vulners.com/exploitdb/EDB-ID:40119> *EXPLOIT*

| EDB-ID:39569 5.5 <https://vulners.com/exploitdb/EDB-ID:39569> *EXPLOIT*

| CVE-2016-3115 5.5 <https://vulners.com/cve/CVE-2016-3115>



192.168.43.240

[FULLSCAN]

2022-07-31 15:57

| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*

| PACKETSTORM:150621 5.0 <https://vulners.com/packetstorm/PACKETSTORM:150621> *EXPLOIT*

| EDB-ID:45939 5.0 <https://vulners.com/exploitdb/EDB-ID:45939> *EXPLOIT*

| EDB-ID:45233 5.0 <https://vulners.com/exploitdb/EDB-ID:45233> *EXPLOIT*

| CVE-2018-15919 5.0 <https://vulners.com/cve/CVE-2018-15919>

| CVE-2018-15473 5.0 <https://vulners.com/cve/CVE-2018-15473>

| CVE-2017-15906 5.0 <https://vulners.com/cve/CVE-2017-15906>

| CVE-2016-10708 5.0 <https://vulners.com/cve/CVE-2016-10708>

| 1337DAY-ID-31730 5.0 <https://vulners.com/zdt/1337DAY-ID-31730> *EXPLOIT*

| CVE-2021-41617 4.4 <https://vulners.com/cve/CVE-2021-41617>

| EDB-ID:40136 4.3 <https://vulners.com/exploitdb/EDB-ID:40136> *EXPLOIT*

| EDB-ID:40113 4.3 <https://vulners.com/exploitdb/EDB-ID:40113> *EXPLOIT*

| CVE-2020-14145 4.3 <https://vulners.com/cve/CVE-2020-14145>

| CVE-2016-6210 4.3 <https://vulners.com/cve/CVE-2016-6210>

| 1337DAY-ID-25440 4.3 <https://vulners.com/zdt/1337DAY-ID-25440> *EXPLOIT*

| 1337DAY-ID-25438 4.3 <https://vulners.com/zdt/1337DAY-ID-25438> *EXPLOIT*

| CVE-2019-6110 4.0 <https://vulners.com/cve/CVE-2019-6110>

| CVE-2019-6109 4.0 <https://vulners.com/cve/CVE-2019-6109>

| CVE-2018-20685 2.6 <https://vulners.com/cve/CVE-2018-20685>

| SSV:92581 2.1 <https://vulners.com/seebug/SSV:92581> *EXPLOIT*

| CVE-2016-10011 2.1 <https://vulners.com/cve/CVE-2016-10011>

| PACKETSTORM:151227 0.0 <https://vulners.com/packetstorm/PACKETSTORM:151227> *EXPLOIT*

| PACKETSTORM:140261 0.0 <https://vulners.com/packetstorm/PACKETSTORM:140261> *EXPLOIT*

| PACKETSTORM:138006 0.0 <https://vulners.com/packetstorm/PACKETSTORM:138006> *EXPLOIT*

| PACKETSTORM:137942 0.0 <https://vulners.com/packetstorm/PACKETSTORM:137942> *EXPLOIT*

| 1337DAY-ID-30937 0.0 <https://vulners.com/zdt/1337DAY-ID-30937> *EXPLOIT*

80/tcp open http Golang net/http server (Go-IPFS json-rpc or InfluxDB API)