

When Bitcoin Core automatically opens outgoing P2P connections, it chooses a peer (address and port) from its list of potential peers. This list is populated with unchecked data gossiped over the P2P network by other peers.

A malicious actor may gossip an address:port where no Bitcoin node is listening, or one where a service is listening that is not related to the Bitcoin network. As a result, this service may occasionally get connection attempts from Bitcoin nodes.

"Bad" ports are ones used by services which are usually not open to the public and usually require authentication. A connection attempt (by Bitcoin Core, trying to connect because it thinks there is a Bitcoin node on that address:port) to such service may be considered a malicious action by an ultra-paranoid administrator. An example for such a port is 22 (ssh). On the other hand, connection attempts to public services that usually do not require authentication are unlikely to be considered a malicious action, e.g. port 80 (http).

Below is a list of "bad" ports which Bitcoin Core avoids when choosing a peer to connect to. If a node is listening on such a port, it will likely receive fewer incoming connections.

```
1:      tcpmux
7:      echo
9:      discard
11:     systat
13:     daytime
15:     netstat
17:     qotd
19:     chargen
20:     ftp data
21:     ftp access
22:     ssh
23:     telnet
25:     smtp
37:     time
42:     name
43:     nickname
53:     domain
69:     tftp
77:     priv-rjs
79:     finger
87:     ttylink
95:     supdup
101:    hostname
102:    iso-tsap
103:    gppitnp
104:    acr-nema
109:    pop2
110:    pop3
111:    sunrpc
113:    auth
115:    sftp
117:    uucp-path
119:    nntp
123:    NTP
135:    loc-srv /epmap
137:    netbios
139:    netbios
```

```
143:  imap2
161:  snmp
179:  BGP
389:  ldap
427:  SLP (Also used by Apple Filing Protocol)
465:  smtp+ssl
512:  print / exec
513:  login
514:  shell
515:  printer
526:  tempo
530:  courier
531:  chat
532:  netnews
540:  uucp
548:  AFP (Apple Filing Protocol)
554:  rtsp
556:  remotefs
563:  nntp+ssl
587:  smtp (rfc6409)
601:  syslog-conn (rfc3195)
636:  ldap+ssl
989:  ftps-data
990:  ftps
993:  ldap+ssl
995:  pop3+ssl
1719: h323gatestat
1720: h323hostcall
1723: pptp
2049: nfs
3659: apple-sasl / PasswordServer
4045: lockd
5060: sip
5061: sips
6000: X11
6566: sane-port
6665: Alternate IRC
6666: Alternate IRC
6667: Standard IRC
6668: Alternate IRC
6669: Alternate IRC
6697: IRC + TLS
10080: Amanda
```

For further information see:

[pull/23306](#)

[pull/23542](#)

fetch.spec.whatwg.org

chromium.googlesource.com

hg.mozilla.org