

Forum:[Hack Forums](#)

Thread: [port tcp/30102 open?](#)

FrankMurphy31 - November 16, 2018, 8:43 pm

I ran an nmap scan on my android and tcp port 30102 is open. Why is this port open? I ran scans in the past on my android and this port was not open. I did a google search and this is what i got:

Port 30102 Details

known port assignments and vulnerabilities

threat/application/port search:

search

Port(s) Protocol Service Details Source

30102 tcp trojan [trojan] NetSphere Trojans

30102 tcp NetSphere [trojan] NetSphere SANS

30102 tcp threat RAT: NetSphere (TCP) An FTP service is run at TCP port 30102 in order to download screen captures. Bekkoame

30100-30103 tcp trojan NetSphere trojan uses these ports.

30100 tcp - the main port that NetSphere connects to.

30101-30103 tcp - NetSphere runs FTP services on these ports, used to transfer various files (e.g. keylog files).

NetSphere infects only Windows 9x systems. A server program called nssx.exe is placed in the C:\Windows\System directory, a "NSSX" value is added to the Run hive of the registry to launch the server.

Port 30100 is IANA registered for Remote Window Protocol (TCP/SCTP) SG

30101-30259 tcp,udp Unassigned IANA

I can connect to this port using netcat but dont know where to go from there to figure out why its open or what service is running on it. Im guessing FTP but i still need to do further research.RAT Netsphere? as in Remote Access Tool?Im confused. is there a backdoor on my phone or something? Any answers or input would be appreciated. Thank you.

sh4moon - November 17, 2018, 7:29 pm

I had something similar happen recently. a port opened up on two different android devices on my network out of nowhere. they were small web servers somehow connected to Netflix.

see how it responds to different things. also, I've used that port site you're talking about. it associates almost every port with some kind of malware. probably nothing to worry about.

FrankMurphy31 - November 17, 2018, 9:48 pm

Thanks for the reply sh4moon. Im going to look further into it but your probably right about nothing to worry about. Oddly though this port opened up soon after I connected to an ssh server on my android, so Im wondering if this has any association.

fattypouches - November 18, 2018, 9:55 pm

did you try to nmap -O the port?

If so, I'd recommend busting out some python and sending different packets to the port to see what

you get.

FrankMurphy31 - November 18, 2018, 10:02 pm

No i have not tried -O on the port yet. I definetly will give it a try though.

[BLANK] - November 19, 2018, 2:12 pm

Since it is an unregistered port it could be used for anything. Best would be to run a packet capture and see what is going over the port.

FrankMurphy31 - November 19, 2018, 9:11 pm

Thanks for the input. Ill ssh into my android and run Wireshark.

CyberStrike - November 21, 2018, 7:10 pm

(Nov 19, 2018 03:12 PM)[BLANK] Wrote: [\[CITE\]](#) Since it is an unregistered port it could be used for anything. Best would be to run a packet capture and see what is going over the port.

+1 This is exactly what I would do myself, at the very least you can have an idea of where it's connecting, maybe intercept some of the traffic you then can look up those IP's in threat feeds and get an idea if it's been seen before. If it's rooted which is sounds like check out lsof with grep for that port.

HangMansheart - November 23, 2018, 1:35 am

Some installed apps just open up random high # ports in order to avoid clogging up your connections. Otherwise, could be a trojan if you've installed any unverified apks