Terramaster NAS exposing itself with UPNP

The Terramaster NAS decided to expose itself to the public internet without asking. Let's see what we can do about it.

POSTS

Terramaster NAS exposing itself with UPNP

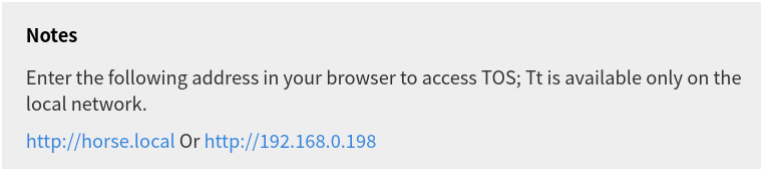
By **Kevin Norman**

April 3, 2021 - 4 minutes read - 789 words

HN | Reddit

> Addendum: The most controversial detail in this blog post so far has been my claim that disabling uPnP is a significant hit to convenience. I wanted to be fully transparent and say that I do not have data to back this claim up, and this is more of a feeling than it is an analytical decision. This criticism somewhat misses the point however, since the vast majority of consumer routes I've encountered personally have uPnP enabled by default, and the consumers purchasing this NAS might have no idea what uPnP is or how to disable it. I plan a blog post in future where I will disable uPnP without making any other changes, to see if anything breaks at all, because it is completely possible my opinion on this is wrong.
>
> I have released another blog post related to this one, which provides more detail: Ok, Ok, I'm Turning uPnP off.
>
> Terramaster appear to have released a fix for this, although I have not tested it yet. Read more

I recently bought a Terramaster F2-210. It's a reasonably nice NAS that does what I ask of it. I however discovered something which unsettled me. As I've discussed in previous articles uPnP is a convenience that can be particularly dangerous. These NAS products are generally administrated using a web interface and The Terramaster TOS software is no different. The software requests you visit the hostname of the device on your network port 8181 in order to access the NAS interface, and the interface openly claims the NAS is not publicly accessible.



A few days after installing the NAS, I discovered I could access the NAS using my public IP, even though I hadn't port forwarded anything! Upon inspecting my routers port forwarding rules, I identified that the NAS was punching 4 ports using uPnP. It was punching 8181 as we just discovered, but also 5443 which is for SSL access should you have configured it, and inexplicably port 9091, which normally is for Portainer, a container management tool for Docker, as well as 8800 - I'm not sure what this port is. It seems that potentially some of these rules were left in from the development process. I trust this NAS to be reliable hardware, however I am dubious of trusting its web interface to the open internet. Generally good practice to expose as little as possible to the public internet anyway!

TCP	5443	5443	0.0.0.0	192.168.0.198	http_ssl
TCP	8181	8181	0.0.0.0	192.168.0.198	http
TCP	9091	9091	0.0.0.0	192.168.0.198	pt
TCP	8800	8800	0.0.0.0	192.168.0.198	http_pri

Unfortunately, disabling uPnP these days is too much of a hit to convenience, so I looked for other solutions. My router is an ISP provisioned one so the feature-set there is somewhat limited, so I wanted to prevent the NAS from opening these ports rather than firewalling them off at the router.

I dug through the NAS interface and was not able to discover a way to disable this behaviour, since I didn't really want my NAS administration interface publicly accessible. What I did discover was that the default web server port was at least configurable, so I changed it, and checked the uPnP port mappings again. Somewhat surprisingly, it punched holes for these new ports, but didn't clear the existing ports! The NAS uPnP rules it punches are 5443, 8181, 9091, 8800, 54633, and 54632".

Protocol	WAN port	LAN port	Destination	Description
UDP	9308	9308	192.168.0.26	192.168.0.26:9308 to 9308 (UDP)
TCP	5443	5443	192.168.0.198	http_ssl
TCP	8181	8181	192.168.0.198	http
TCP	9091	9091	192.168.0.198	pt
TCP	8800	8800	192.168.0.198	http_pri
UDP	6672	6672	192.168.0.26	NAT-PMP 6672 udp
TCP	54633	54633	192.168.0.198	http_ssl
TCP	54632	54632	192.168.0.198	http

This annoyed me, so I contacted Terramaster about this 6 weeks ago, hoping they'd have a suggestion or something as a fix, but this wasn't supplied, and therefore I went digging myself.

Upon SSHing into the NAS and having a dig around the file system, I discovered a file that could be modified. /etc/upnp.json seems to contain a list of port forwarding rules. Thank you to Terramaster for providing root access to these at least. Simply change `bEnable` to 0 for whatever ports you don't want exposed, reboot the NAS, and check the port forwarding rules.


```
"triestimes": 3,
"mapList": [
    {
        "desc": "ftp",
        "nExternalPort": 6221,
        "nInternalPort": 21,
        "sProtocol": "TCP",
        "bEnable": 0
    },
    {
        "desc": "ftp_data",
        "nExternalPort": 2000,
        "nInternalPort": 20,
        "sProtocol": "TCP",
        "bEnable": 0
    },
    {
        "desc": "sshd",
        "nExternalPort": 22,
        "nInternalPort": 22,
        "sProtocol": "TCP",
        "bEnable": 1
    },
    {
        "desc": "telnetd",
        "nExternalPort": 23,
        "nInternalPort": 23,
        "sProtocol": "TCP",
        "bEnable": 0
    },
    {
```

```
            "desc": "http_ssl",
            "nExternalPort": 54633,
            "nInternalPort": 54633,
            "sProtocol": "TCP",
            "bEnable": 0
        },
        {
            "desc": "http",
            "nExternalPort": 54632,
            "nInternalPort": 54632,
            "sProtocol": "TCP",
            "bEnable": 0
        },
        {
            "desc": "pt",
            "nExternalPort": 9091,
            "nInternalPort": 9091,
            "sProtocol": "TCP",
            "bEnable": 0
        },
        {
            "desc": "http_pri",
            "nExternalPort": 8800,
            "nInternalPort": 8800,
            "sProtocol": "TCP",
            "bEnable": 0
        }
    ]
```


result in a 404, since we moved the web server earlier. This is better than before, but still not perfect. I'll further instructions from Terramaster/a software update, and will update this blog post should I get this.

HN | Reddit

Let me know what you thought! Tweet me at @normankev141

software badideas

Related

Exploiting UPnP, Literally Childsplay.
Declouding my life - Replacing Google Photos
Declouding Chinese WIFi plugs
Improving Bluetooth Audio Quality on Ubuntu Linux
Why Does My Computer Not Boot with a USB Hub Attached?
Embedded Meets the Internet: Build Your Own Air Quality Meter
Gnome Shell Stuttering Caused by AppIndicator
How Do I Make Breaking Changes in Go Without Annoying People?
Beating Round-Trip Latency With Redis Pipelining
News in the Morning: A Simple Hack
NotSoEducated – A Project From a While Ago