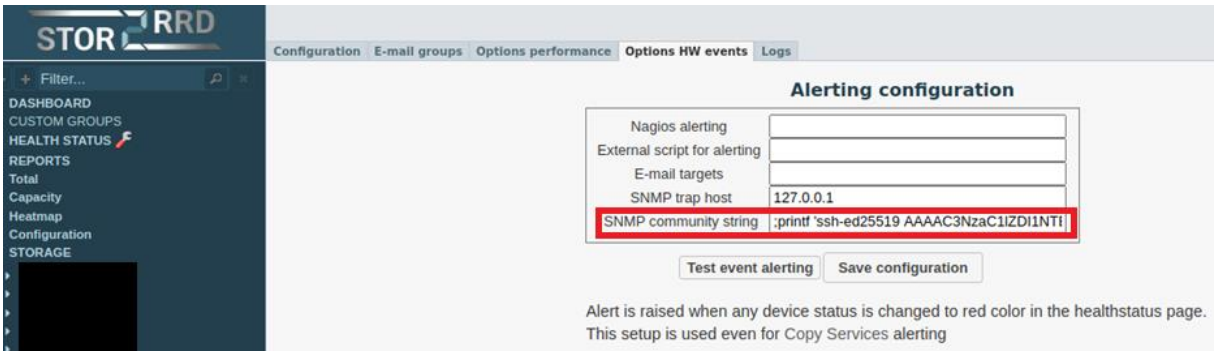
Vulnerability #1: Remote command injection

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

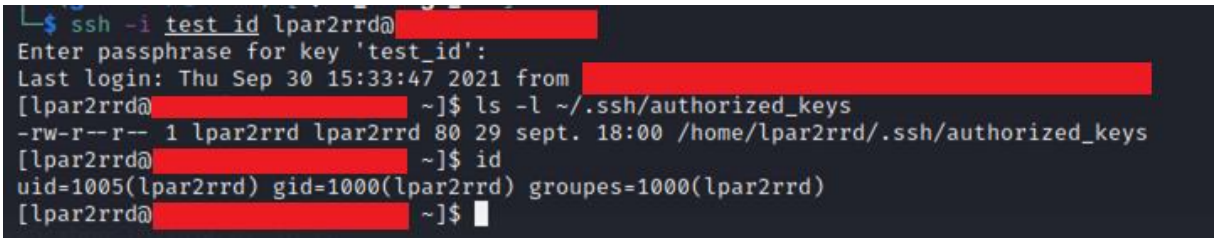
A shell command injection in HW Events SNMP community string in XoruX STOR2RRD allows authenticated remote attackers to execute arbitrary shell commands as the user running the service.

- Injected command : `;printf 'ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAA' >~/.ssh/authorized_keys#`



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

- Opening a shell using the uploaded SSH authorized key:



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.