Zyxel NAS326 Issues

Cannot login to web after upgrade

NAS326 with FFP and other mods survives official upgrade, but it is not possible to login using web. Login using SSH works.

Zyxel explains it: Not able to login after Firmware Upgrade

```
To avoid the remote code execution vulnerability, the password doesn't
accept special characters !  #  $  %  &  (  -  | after updated to the latest
firmware.
If you cannot login the web interface after upgrade, please press the
hardware reset button at the back of NAS for 2 seconds, and you will hear
one beep sound,
then release the hardware reset button. This resets the NAS's IP address and
password to the default setting (admin/1234).
```

Zyxel security advisory for the remote code execution vulnerability of NAS products

Additional findings:

- It looks like, webui is using smbpasswd to authenticate to webinterface
- When the reset button is pressed shortly, script to restore default passwords is called:

| /sbin/account.sh

```sh
#!/bin/sh

CP=/bin/cp
RM=/bin/rm
ETCPATH=/etc
SAMBAPATH=/etc/samba

${RM} -rf /etc/passwd
${CP} ${ETCPATH}/passwd.default /etc/passwd
${RM} -rf  /etc/shadow
${CP} ${ETCPATH}/shadow.default /etc/shadow
${RM} -rf /etc/samba/smbpasswd
${CP} ${SAMBAPATH}/smbpasswd.default /etc/samba/smbpasswd
```

From:
https://niziak.spox.org/wiki/ - **niziak.spox.org**

Permanent link:
https://niziak.spox.org/wiki/hw:zyxel_nas326:issues

Last update: **2020/04/22 09:12**