Node Server Security Update Guide

V1.0

HPB Foundation

October 2018

Contents

Chapter 1 Overview

1.1 Applicable Versions

This Guide is applicable to HPB node servers running Linux operation systems. Based on the Designated Server Security Update Plan and in order to improve security for HPB node servers, it is aimed at helping our node users carry out security compliance checks and securely configure their servers.

1.2 Reading Guide

No.	Contents	Descriptions
1	User guide of the script for server security check	Guidance for node users to download, operate script for server security check and check security configuration of the server. See Chapter 2 for details.
2	Details of item testing	Detailed description of 22 items for testing involving in the script and steps of their configuration modification. See Chapter 3 for details.

Chapter 2 User Guide for Script of Server Security Detection

2.1 Step-by-Step Instruction

To simplify the operation process for our users, we provide the script for server security checks that will automatically carry out sercurity configuration checks on the server’s Linux system.

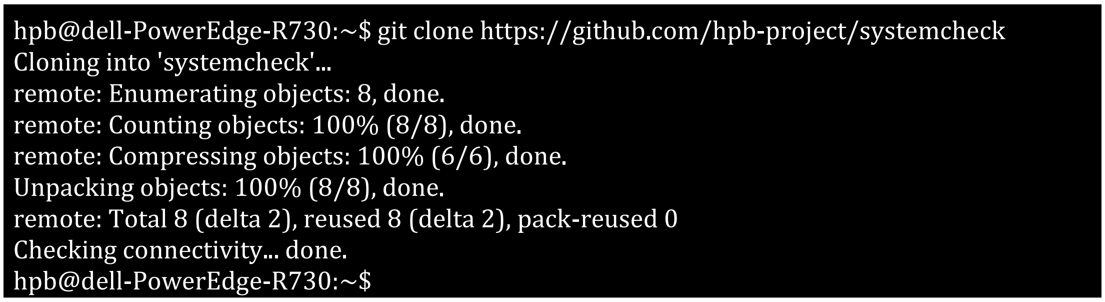
No.	Steps	Descriptions
1	Download the script	Command: ”**git clone** *https://github.com/hpb-project/systemcheck*”
2	Set permission	Command: ”**cd** *systemcheck*” Command: ”**chmod +x** *systemcheck.sh*”
3	Run the script	Command: ”**sudo** *./systemcheck.sh*” **Tip**: Users are required enter their password as prompted to log in their current account; When it shows ”You haven’t installed chkconfig, install now (y/n)”， enter ”y”.
4	Check results	Command: ”**vi** *servercheck.txt*” **Tip**: Items that passed the check are prompted as ”safe”. Failed to pass are prompted as ”unsafe”. See Chapter 3 to see whether it is mandatory to change configuration settings. (E.g. For item no.1, check Chapter 3.1; for item number no.2, check Chapter 3.2, etc.)

We suggest you change the configuration of items that failed to pass the check into security configuration. See Chapter 3 for detailed steps.

2.2 Example

(1) Download the script for the server security check

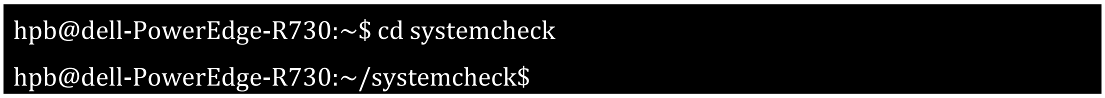
Open the terminal, enter ”**git clone** *https://github.com/hpb-project/systemcheck*”;



```
hpb@dell-PowerEdge-R730:~$ git clone https://github.com/hpb-project/systemcheck
Cloning into 'systemcheck'...
remote: Enumerating objects: 8, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
Unpacking objects: 100% (8/8), done.
remote: Total 8 (delta 2), reused 8 (delta 2), pack-reused 0
Checking connectivity... done.
hpb@dell-PowerEdge-R730:~$
```

(2) Set file permissions

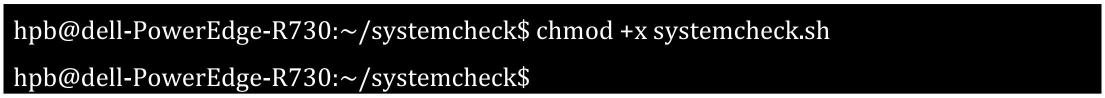
Enter ”**cd** *systemcheck*”



```
hpb@dell-PowerEdge-R730:~$ cd systemcheck
hpb@dell-PowerEdge-R730:~/systemcheck$
```

Continue to set file permissions

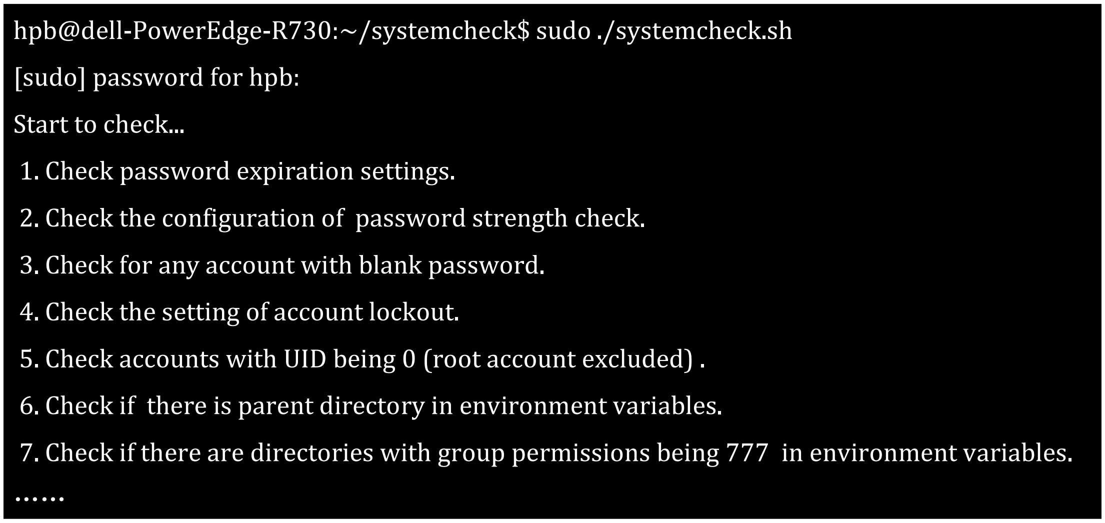
Enter ”**chmod +x** *systemcheck.sh*”



```
hpb@dell-PowerEdge-R730:~/systemcheck$ chmod +x systemcheck.sh
hpb@dell-PowerEdge-R730:~/systemcheck$
```

(3) Run the script

Enter ”**sudo** *./systemcheck.sh*” then enter password as prompted to log in to the current account. Server configuration will be checked automatically.



```
hpb@dell-PowerEdge-R730:~/systemcheck$ sudo ./systemcheck.sh
[sudo] password for hpb:
Start to check...
 1. Check password expiration settings.
 2. Check the configuration of  password strength check.
 3. Check for any account with blank password.
 4. Check the setting of account lockout.
 5. Check accounts with UID being 0 (root account excluded) .
 6. Check if  there is parent directory in environment variables.
 7. Check if there are directories with group permissions being 777  in environment variables.
……
```

When prompted ”You haven’t installed chkconfig, install now (y/n) :”, enter ”y” to install **chkconfig**; when it shows ”Completed, please read file **servercheck.txt**”, the security detection is completed.

```
19. Check the running services
19. You haven’t installed chkconfig, install now (y/n) :y
Reading package lists... Done
Building dependency tree
Reading state information... Done
……
Setting up sysv-rc-conf (0.99-7) ...
Install Success!
20. Check the status of core dump
Check is completed, please read file servercheck.txt
```

(4) Check the running results

Enter ”**vi** *servercheck.txt*” and the system will show the running results, there are 22 items in total for check in the results, items that have passed the check are prompted as ”safe”， failed to pass are prompted as ”unsafe”. We suggest you change the configuration of items that failed to pass the check into security configuration. See Chapter 3 for detailed steps.

(e.g. For item no.1, check Chapter 3.1; for item number no.2, check Chapter 3.2, etc.)

```
hpb@dell-PowerEdge-R730:~/systemcheck$ vi servercheck.txt
1. Unsafe: you haven’t set password timeout time
Suggestion:
  Execute ‘sed -i '/PASS_MAX_DAYS/s/99999/90/g' /etc/login.defs’ to set  your password
expiration of 90 days.
2. Unsafe: you haven’t set up password strength check
Suggestion:
  Execute ‘echo "passwd requisite pam_cracklib.so difok=3 minlen=8 ucrediit=-1 lcredit=-1
dcredit=-1">> /etc/pam.d/
systemd-auth’ to set your passwords with required capital and lowercase letters and numbers.
The minum length of your password should be 8 digits.
3. Safe: no account with blank password has been found
```

Chapter 3 Details of items for check

3.1 Set Password Expiration

3.1.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Set password expiration (of 90 days)	Command: ” **sed -i** *'/PASS_MAX_DAYS/s/99999/90/g'* */etc/login.defs*”

3.1.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Set password expiration

Enter ”**sed -i** *'/PASS_MAX_DAYS/s/99999/90/g' /etc/login.defs*” to set your password expiration of 90 days. There is no message returned for this command.

```
root@dell-PowerEdge-R730:/home/hpb# sed -i '/PASS_MAX_DAYS/s/99999/90/g'
/etc/login.defs
```

3.2 Configure Password Strength Check

3.2.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Configure password strength check	Command: ”**echo** *"passwd requisite pam_cracklib.so difok=3 minlen=8 ucrediit=-1 lcredit=-1 dcredit=-1">> /etc/pam.d/systemd-auth*”

3.2.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user.

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Configure password strength check

Enter ” **echo** *"passwd requisite pam_cracklib.so difok=3 minlen=8 ucrediit=-1 lcredit=-1 dcredit=-1">> /etc/pam.d/systemd-auth* ” to set your passwords with required capital and lowercase letters and numbers. The minum length of your password should be 8 digits. There is no message returened for this command.

```
root@dell-PowerEdge-R730:/home/hpb#  echo "passwd requisite pam_cracklib.so difok=3
minlen=8 ucrediit=-1 lcredit=-1 dcredit=-1">> /etc/pam.d/systemd-auth
root@dell-PowerEdge-R730:/home/hpb#
```

3.3 Account with Blank Password

3.3.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Set account password	Command: ”**passwd** *user name*” **Tip**: Change the user name into one that you haven’t set password for; Enter and re-enter your new passwords as prompted

3.3.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user.

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Set account password

Enter ”**passwd** *user name*”, enter new password as prompted, then re-enter the password to complete the setting.

Tip: Change the user name into one that you haven’t set password for, the account name in the example below is ”test”.

```
root@dell-PowerEdge-R730:/home/hpb# passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

3.4 Set Account Lockout

3.4.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you are logged in as root user)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Set account lockout	Command: ”**echo** *"auth required pam_tally.so onerr=fail deny=10 unlock_time=300" >> /etc/pam.d/systemd-auth*””

3.4.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user.

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Set account lockout

Enter ”**echo** *"auth required pam_tally.so onerr=fail deny=10 unlock_time=300" >> /etc/pam.d/systemd-auth* ” to set account lockout after 10 failed password attempts in a row. There is no returned message for this command;

Command to unlock the account: ”**faillog -u** *<user>* **-r**”.

```
root@dell-PowerEdge-R730:/home/hpb#  echo "auth required pam_tally.so onerr=fail
deny=10 unlock_time=300" >> /etc/pam.d/systemd-auth
root@dell-PowerEdge-R730:/home/hpb#
```

3.5 Account with UID being 0

3.5.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you've already done so)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Change to the name of an account with UID being 0	Command: ” **usermod -u** *<new-uid> <user>*” Command: ” **groupmod -g** *<new-gid> <user>*”

3.5.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user.

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Change to the name of an account with UID being 0

Enter ”**usermod -u** *<new-uid> <user>*”; then enter ”**groupmod -g** *<new-gid> <user>*”.

Tip: Change '<user>' to the name of an account with UID being 0; replace '<new-uid>' with new uid; '<new-gid>' is to show parameter.

3.6 Parent Directory in Environment Variables

We suggest you change the configuration and remove the parent directory from environment variables if there is any.

3.7 Directories with Group Permissions Being 777 in Environment Variables

If there are directories with group permissions being 777 in environment variables, we suggest you execute chmod command to change the directory permission in running results.

3.8 Remote Connection Security

If remote connection security failed to pass the check, we suggest you check with the administrator whether files shown in the running results should be deleted.

3.9 Umask Configuration

3.9.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” `su root`” **Tip**: Enter your root account password as prompted
2	For ‘umask’ unconfigured	Command: ”**echo** *"umask 027" >> /etc/profile*” Command: ”**echo** *"umask 027" >> /etc/bash.bashrc*”
2’	For ‘umask’ with unsafe configuration	Command: ”**vi** */etc/profile*” Find out the ‘umask’ parameter and change the numbers to ”027” Command: ”**vi** */etc/bash.bashrc*” Find out the umask parameter and change the numbers to ”027”

3.9.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user.

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) For ‘umask’ unconfigured

Enter ”**echo** *"umask 027" >> /etc/profile*”, there is no message returned for this command;

Enter ”**echo** *"umask 027" >> /etc/bash.bashrc*”, there is no message returned for this command;

```
root@dell-PowerEdge-R730:/home/hpb#  echo "umask 027" >> /etc/profile
root@dell-PowerEdge-R730:/home/hpb# echo "umask 027" >> /etc/bash.bashrc
```

(3) For ‘umask’ with unsafe configuration

Enter ”**vi** */etc/profile*”; press the direction key ” ↓ ” to move the cursor to umask parameter, then change the numbers to ”027”;

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/profile
if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
umask 027
TMOUT=180

:wq（Press the key ”ESC”, then enter ”:wq” to save the file before you exit.）
```

Enter ”**vi** */etc/bash.bashrc*”

Press the direction key ” ↓ ” to move the cursor to umask parameter, then change the numbers to ”027”;

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/bash.bashrc
if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
umask 027
TMOUT=180

:wq（Enter the key ”ESC”, then enter ”:wq” to save the file before you exit.）
```

3.10 Permissions of Key Files and Directories

Check the files and directories in the running results and upgrade the low permissions as soon as possible.

3.11 Unauthorized File SUID/SGID

Check for any suspicious directory/file in the running results and delete accordingly.

3.12 Permission to Write Directory

Check in the running results if the permission to write directory is accessible to everyone, change the permission as necessary.

3.13 Permission to Write File

Check in the running results if the permission to write directory is accessible to everyone, change the permission as necessary.

3.14 File of No Owner

For files of no owners in the running results, add owners or delete them if they turn out to be suspicious files.

3.15 Exceptional File

Check in the running results if the file is suspicious and delete accordingly.

3.16 Configure Log-in Timeout

3.16.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Add configuration of login timeout	Command: ”**echo** *"TMOUT=180" >> /etc/profile*”

3.16.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user.

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Add configuration of login timeout

Enter ”**echo** *"TMOUT=180" >> /etc/profile*”, there is no message returned for this command;

```
root@dell-PowerEdge-R730:/home/hpb#  echo "TMOUT=180" >> /etc/profile
root@dell-PowerEdge-R730:/home/hpb#
```

3.17 Running Status of ssh and telnet

If ssh is not in running status, we suggest you install and run this service;

If telnet is in running status, we suggest you stop this service.

3.18 Permit Root Remote Login

3.18.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” `su root`” **Tip**: Enter your root account password as prompted
2	Permit remote root login	Command: ” **vi** */etc/ssh/sshd_config*” Find out parameter ”PermitRootLogin”, then change the ”yes” to ”no”. **Tip**: No change is needed for information other ”yes” in the parameter.

3.18.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Permit remote root login

Enter”**vi** */etc/ssh/sshd_config*”, move the cursor to find out the parameter ’PermitRootLogin’ in the opened file, change the ”yes” to ”no”.

Tip: No change is needed for information other ”yes” in the parameter.

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/ssh/sshd_config

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes

:wq（Enter the key ”ESC”, then enter ”:wq” to save the file before you exit.）
```

3.19 Running Services

Check for services that are running and close the unnecessary ones.

Command to close the service ”**chkconfig --level $level** <*name of service*> ”

3.20 Core dupm Status

3.20.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Modify the file ‘limits’	Command: “**vi** */etc/security/limits.conf*” Enter the following codes before ”End of file” “* soft core 0 * hard core 0”

3.20.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Modify the file ‘limits’

Enter ”**vi** */etc/security/limits.conf*”;

Move the cursor to the line of codes ahead of”End of file”,

```
Enter   ”* soft core 0
          * hard core 0”.
```

Tip: If you fail to enter the codes, press the key of letter ”I” to start ”INSERT” input state.

```
root@dell-PowerEdge-R730:/home/hpb#

#ftp            hard    nproc           0
#ftp            -       chroot          /ftp
#@student       -       maxlogins       4
* soft core 0
* hard core 0
# End of file
:wq（Press the key ” ESC” , then enter ” :wq” to save the file before you exit.）
```

3.21 Rsyslog Status

3.21.1 Step-by-Step Instruction

No.	Steps	Descriptions
1	Switch to root user (Skip this step if you’ve already done so)	Command: ” **su** root” **Tip**: Enter your root account password as prompted
2	Configure and start ‘rsyslog’	Command: ”**vi** */etc/rsyslog.conf*”; Enter the codes below at the end of the file: ”***.err;kern.debug;daemon.notice /var/adm/messages**” Command: ”**sudo mkdir** */var/adm*” Command: ”**sudo touch** */var/adm/messages*” Command: ”**sudo chmod 666** */var/adm/messages*” Command: ”**sudo systemctl restart** *rsyslog*”

3.21.2 Example

(1) Switch to root user

Open the terminal, enter ”**su** root” then enter your root account password as prompted;

Tip: Skip this step if you already switched to root user

```
hpb@dell-PowerEdge-R730:~$ su root
Password:
root@dell-PowerEdge-R730:/home/hpb#
```

(2) Configure and start ‘rsyslog’

Enter ”**vi** */etc/rsyslog.conf*” to open the file ‘rsyslog.conf’;

Press the key of letter”I” to start ”INSERT”input state.

Press the direction key ” ↓ ” to move the cursor the the last line and enter:

”***.err;kern.debug;daemon.notice /var/adm/messages**”;

Press the key ”ESC”, then enter ”**:wq**” to save the file beforeyou exit;

```
root@dell-PowerEdge-R730:/home/hpb# vi /etc/rsyslog.conf


#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.err;kern.debug;daemon.notice /var/adm/messages


:wq（Press the key ” ESC” , then enter ” :wq” to save the file and exit）
```

Continue to enter ”**sudo mkdir** */var/adm* ”, no message is returned for this command;

Then enter ”**sudo touch** */var/adm/messages*”, no message is returned for this command;

Then enter ”**sudo chmod 666** */var/adm/messages*”, no message is returned for this command;

Then enter ”**sudo systemctl restart** *rsyslog*”, no message is returned for this command;

```
root@dell-PowerEdge-R730:/home/hpb# sudo mkdir /var/adm
root@dell-PowerEdge-R730:/home/hpb# sudo touch /var/adm/messages
root@dell-PowerEdge-R730:/home/hpb# sudo chmod 666 /var/adm/messages
root@dell-PowerEdge-R730:/home/hpb# sudo systemctl restart rsyslog
```

3.22 BOE Function Compatibility Testing

Skip this test if you haven’t installed the server of BOE hardware unit;

If you are required to pass this test but failed, please contact our staff through ‘Annex Technical Support’ and provide the system message shown in the running results for further technical assistance.

Annex Technical Support

If you require further technical assistance, please contact our HPB Staff by one of the following methods:

Hot Line Service: +86 021-5895 9195（China）

E-mail: node@hpb.io

HPB Technical Community: http://blockgeek.org/

HPB Official Website: http://www.hpb.io/

Telegram: https://t.me/hpbglobal

Facebook: HPB Blockchain

Twitter: @HPBGlobal

Reddit: r/HPBGlobal