Security problem of zabbix-agent2

There is a security problem with zabbix-agent2. zabbix-agent2-openrc package.

Old zabbix_agentd works correctly under "$user" zabbix which is set by /etc/zabbix/zabbix_agentd.conf

```
2929 zabbix     0:00 /usr/sbin/zabbix_agentd -f
2955 zabbix    31:09 /usr/sbin/zabbix_agentd: collector [idle 1 sec]
2958 zabbix     2:34 /usr/sbin/zabbix_agentd: listener #3 [waiting for connecti
```

But "$user" in zabbix-agent2 is set not in config file(/etc/zabbix/zabbix_agent2.conf), but in systemd , which is absent in alpine (and this is good).

It should be section of setting "$user" in /etc/init.d/zabbix-agent2 for starting zabbix-agent2, otherwise it is executed (started) under root.

```
20950 root       0:00 supervise-daemon zabbix-agent2 --start /usr/sbin/zabbix_agent2 --
20951 root       0:00 /usr/sbin/zabbix_agent2
```

It is possible to get root access in client potentially during data transfer through public networks with default settings when using zabbix-agent2.

To upload designs, you'll need to enable LFS and have an admin enable hashed storage. **More information**

Child items ◎ 0	

No child items are currently assigned. Use child items to prioritize tasks that your team should complete in order to accomplish your goals!

Linked items ❔ 🗋 0	

Related merge requests ⑂ 1
⑃ **community/zabbix: run agent2 as zabbix user**
!29089   ⊘

When this merge request is accepted, this issue will be closed automatically.

🏷 **Kevin Daudt** 🖥 **@kdaudt** added tag:security label 10 months ago

👤 **Kevin Daudt** 🖥 **@kdaudt** assigned to **@kdaudt** 10 months ago

💬 **Kevin Daudt** 🖥 **@kdaudt** mentioned in merge request !29089 (merged) 10 months ago

⊖ **Kevin Daudt** 🖥 **@kdaudt** closed via merge request !29089 (merged) 10 months ago

💬 **Kevin Daudt** 🖥 **@kdaudt** mentioned in commit 0bd3b989 10 months ago

💬 **Kevin Daudt** 🖥 **@kdaudt** mentioned in commit 7b9f3ca0 10 months ago

Kevin Daudt 🖥 **@kdaudt** · 10 months ago   (Owner)
Thanks for reporting. I've fixed it and backported the fix to 3.15 and 3.14.

Kevin Daudt 🖥 **@kdaudt** · 10 months ago   (Owner)
CVE-2022-22704 has been assigned for this

Please register or sign in to reply