Bug 3690 - sshd: root [priv] process sleeping leads to unprivileged child proc zombie

Status: RESOLVED DUPLICATE of bug 3598

Alias: None

Product: Portable OpenSSH
Component: sshd (show other bugs)
Version: 8.5p1
Hardware: All Linux

Importance: P5 normal
Assignee: Assigned to nobody

URL:
Keywords:

Depends on:
Blocks:

Reported: 2024-05-13 00:19 AEST by linker
Modified: 2024-07-02 05:51 AEST (History)
CC List: 4 users (show)

See Also:

Attachments		
deadlock process call stack (3.17 KB, text/plain) 2024-05-13 00:19 AEST, linker	*no flags*	Details
Add an attachment (proposed patch, testcase, etc.)		View All

Note
You need to log in before you can comment on or make changes to this bug.

linker 2024-05-13 00:19:08 AEST Description

```
Created attachment 3814 [details]
deadlock process call stack

In the `sshd.c` file, the `grace_alarm_handler()` signal handling function calls
`sigdie()`, which in turn calls `sshsigdie()`, and within this call, functions such
as `shlogv()`, `do_log()`, `{openlog(), syslog(), closelog()}` are invoked.
Similarly, within the main thread, the `privsep_preauth()` function calls
`monitor_child_preauth()`, which then calls `auth_log()`, and this also results in
calls to `{openlog(), syslog(), closelog()}`.

Since these functions are not async-signal-safe and they utilize a global lock
named `syslog_lock`, this can lead to a recursive deadlock (AA lock). As a result,
the pre-authentication process may end up in a zombie state and fail to exit.
```

Damien Miller 2024-05-13 21:01:40 AEST Comment 1

```
*** This bug has been marked as a duplicate of bug 3598 ***
```

Format For Printing - XML - Clone This Bug - Top of page