Bug 1245759 - Attach-process does not work. "ptrace: Operation not permitted"

Keywords:	
Status:	CLOSED CANTFIX
Alias:	None
Product:	Fedora
Component:	eclipse-cdt
Version:	22
Hardware:	Unspecified
OS:	Unspecified
Priority:	unspecified
Severity:	unspecified
Target Milestone:	---
Assignee:	Lev Ufimtsev
QA Contact:	Fedora Extras Quality Assurance
Docs Contact:	
URL:	
Whiteboard:	
Depends On:	1209492
Blocks:	

Reported:	2015-07-22 16:47 UTC by Lev Ufimtsev
Modified:	2015-09-02 18:50 UTC (History)
CC List:	7 users (show)
Fixed In Version:	
Doc Type:	Bug Fix
Doc Text:	
Clone Of:	
Environment:	
Last Closed:	2015-09-02 18:50:17 UTC
Type:	Bug
Dependent Products:	

TreeView+   [depends on](#) / [blocked](#)

[Description](#) Lev Ufimtsev 2015-07-22 16:47:32 UTC
```
Description of problem:
 As of F22, in Eclipse-CDT, you can't debug via "attach to process".
 When you try, nothing happens.

 When trying the same thing with GDB, you get an error:
 "ptrace: Operation not permitted."

 After some troubleshooting, one workaround is:
 sudo chmod +s /usr/bin/gdb

 The root cause of the issue has been narrowed down to a security hardening
in:
 https://bugzilla.redhat.com/show_bug.cgi?id=1209492
 I tested one potential patch and it fixed the issue.
 But at present there is a debate about security in the bug above (50
comments..).
 - The Security-hardening argument is that ptrace has the ability to look
into the memory of any process, thus being a security threat.
 - The usability argument is that the change is security theater. It only
breaks a lot of applications and doesn't really add much security since there
are other easier ways to do the same (e.g core dumping another application
and reading the dump). As such it's fixing something that isn't broken but
causes breakage in many other apps.

 This bug is a tracker bug. It is intended to raise attention that the
security-hardening change (in bug 1209492) breaks Eclipse-cdt's attach-to-
process functionality and imho should be reversed. To me it seems that this
is an unnecessary a big wall that can be easily walked around anyway.



Version-Release number of selected component (if applicable):
 F22. Eclipse independent.

How reproducible:
 Always

Steps to Reproduce:
 - Start a C application. (e.g a JVM).
 - From Eclipse, attempt to attach to the process.

Actual results:
   - Nothing happens

Expected results:
   - Debug session should have started.
```

```
Additional info:
```

Comment 1 Lev Ufimtsev 2015-07-31 22:10:36 UTC
```
It seems the patch is getting reverted. This is good as Eclipse's GDB attach-
to process will continue to function without having to change SELinux
policies.

I'll look into testing things once there is a build available.
```

Comment 2 Lev Ufimtsev 2015-09-02 18:20:27 UTC
```
The child task was closed as WontFix. It's not clear if remote-attach works
on the latest F22/F23 at the moment, I need to test this sometime.
```

Comment 3 Lev Ufimtsev 2015-09-02 18:50:17 UTC
```
After some investigation, the current solution is to install the package:
https://apps.fedoraproject.org/packages/elfutils-default-yama-scope

Which loosens yama scope to allow ptrace and other processes that attach them
selfes to work properly.

The above package has been added as 'weak dedendency' by tools like gdb.
```

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

-
-
-
-
-
-

        -
        -

        -
        - [?]

Type a sub-component name