Ruby - Bug #20527

Control-Flow protection cannot be enabled for Ruby due to ASM bits

06/05/2024 03:39 PM - vo.x (Vit Ondruch)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 3.3.1 (2024-04-23 revision c56cd86388) [x86_64-linux]	**Backport:**	3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN

Description

Checking if Ruby is properly hardened up to Fedora standard using annocheck, this is the result:

```
$ annocheck redhat-linux-build/libruby.so.3.3.1
annocheck: Version 12.54.
Hardened: libruby.so.3.3.1: FAIL: cf-protection test because .note.gnu.property section did not co
ntain the necessary flags
Hardened: libruby.so.3.3.1: FAIL: property-note test because a property note was found but it show
s that cf-protection is not enabled
Hardened: Rerun annocheck with --verbose to see more information on the tests.
Hardened: libruby.so.3.3.1: Overall: FAIL.
```

Wondering what is the issue, I have executed following:

```
$ annocheck redhat-linux-build/* 2>/dev/null | grep FAIL | less
Hardened: Context.o: Overall: FAIL (due to MAYB results).
Hardened: libruby-static.a:Context.o: Overall: FAIL (due to MAYB results).
Hardened: libruby.so.3.3.1: FAIL: cf-protection test because .note.gnu.property section did not co
ntain the necessary flags
Hardened: libruby.so.3.3.1: FAIL: property-note test because a property note was found but it show
s that cf-protection is not enabled
Hardened: libruby.so.3.3.1: Overall: FAIL.
Hardened: miniruby: FAIL: cf-protection test because .note.gnu.property section did not contain th
e necessary flags
Hardened: miniruby: FAIL: property-note test because a property note was found but it shows that c
f-protection is not enabled
Hardened: miniruby: Overall: FAIL.
```

This suggest that the Context.o is the culprit. Lets take a detailed look:

```
$ annocheck redhat-linux-build/coroutine/amd64/Context.o --verbose
annocheck: Version 12.54.
Hardened: redhat-linux-build/coroutine/amd64/Context.o: info: No matching profile found.
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: pie test because the ELF file header
 has the correct type
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: gnu-stack test because non-executabl
e .note.GNU-stack section found
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: gaps test because no notes found - t
herefore there are no gaps!
Hardened: redhat-linux-build/coroutine/amd64/Context.o: MAYB: test: notes, reason: notes not found
 and no DWARF info found (could there be a separate debuginfo file ?)
Hardened: redhat-linux-build/coroutine/amd64/Context.o: info: For more information visit: https://
sourceware.org/annobin/annobin.html/Test-notes.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: bind-now test because only needed fo
r executables
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: branch-protection test because not a
n AArch64 binary
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: cf-protection test because not an x8
6_64 executable
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: dynamic-segment test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: dynamic-tags test because AArch64 sp
ecific
```

```
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: entry test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: fast test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: fips test because not a GO binary
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: fortify test because no compiled C/C
++ code found
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: glibcxx-assertions test because no c
ompiled C/C++ code found
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: gnu-relro test because not needed in
 object files
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: go-revision test because no GO compi
led code found
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: implicit-values test because  These
tests are only relevent to C source code
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: instrumentation test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: lto test because not compiled from C
/C++ code
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: openssl-engine test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: MAYB: test: optimization, reason: could no
t determine how the code was created
Hardened: redhat-linux-build/coroutine/amd64/Context.o: info: For more information visit: https://
sourceware.org/annobin/annobin.html/Test-optimization.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN: This can happen if the program is co
mpiled from a language unknown to annocheck
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN:  or because there are no annobin bui
ld notes (could they be in a separate file ?)
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN: For more details see https://sourcew
are.org/annobin/annobin.html/Absence-of-compiled-code.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: MAYB: test: pic, reason: no valid notes fo
und regarding this test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: info: For more information visit: https://
sourceware.org/annobin/annobin.html/Test-pic.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: production test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: property-note test because property
notes not needed in object files
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: run-path test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: rwx-seg test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: short-enums test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: MAYB: test: stack-clash, reason: could not
 determine how the code was created
Hardened: redhat-linux-build/coroutine/amd64/Context.o: info: For more information visit: https://
sourceware.org/annobin/annobin.html/Test-stack-clash.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN: This can happen if the program is co
mpiled from a language unknown to annocheck
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN:  or because there are no annobin bui
ld notes (could they be in a separate file ?)
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN: For more details see https://sourcew
are.org/annobin/annobin.html/Absence-of-compiled-code.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: MAYB: test: stack-prot, reason: could not
determine how the code was created
Hardened: redhat-linux-build/coroutine/amd64/Context.o: info: For more information visit: https://
sourceware.org/annobin/annobin.html/Test-stack-prot.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN: This can happen if the program is co
mpiled from a language unknown to annocheck
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN:  or because there are no annobin bui
ld notes (could they be in a separate file ?)
Hardened: redhat-linux-build/coroutine/amd64/Context.o: WARN: For more details see https://sourcew
are.org/annobin/annobin.html/Absence-of-compiled-code.html
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: stack-realign test because not an i6
86 executable
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: textrel test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: threads test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: unicode test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: skip: warnings test because no compiled C/
C++ code found
Hardened: redhat-linux-build/coroutine/amd64/Context.o: PASS: writable-got test
Hardened: redhat-linux-build/coroutine/amd64/Context.o: Overall: FAIL (due to MAYB results).
```

Well, skip: cf-protection test because not an x86_64 executable is not really helpful, therefore I have opened ticket with annocheck folks 1, where they suggest to update the Context.S according to the following guidelines:

https://sourceware.org/annobin/annobin.html/Test-cf-protection.html

P.S. With YJIT enabled, there is also issue with the Rust code, therefore I have tested this with YJIT disabled and without Rust available in the environment.

Related issues:

Is duplicate of Ruby - Bug #18061: Execshield test: libruby.so.N.N.N: FAIL: ...	**Closed**

History

#1 - 06/05/2024 04:07 PM - fweimer (Florian Weimer)

The annobin instructions are very misleading for Context.S because it performs stack switching:

```
        # Save caller stack pointer:
        movq %rsp, (%rdi)

        # Restore callee stack pointer:
        movq (%rsi), %rsp
```

This requires extra work: the shadow stack has to be switched as well, and that needs some restore token management. I don't know any writeup of the required steps. We have code for this in glibc (in sysdeps/unix/sysv/linux/x86_64/swapcontext.S), but I don't know the details how it works, sorry.

Shadow stack context switching can be tested on Fedora 40 and later by running on a SHSTK-compatible CPU and setting the GLIBC_TUNABLES=glibc.cpu.hwcaps=SHSTK tunable.

#2 - 06/05/2024 04:38 PM - vo.x (Vit Ondruch)

This is actually duplicate of #18061 (I'll suggest to continue discussion there), which includes this draft implementation:

https://github.com/ruby/ruby/pull/5895

#3 - 06/06/2024 07:53 PM - alanwu (Alan Wu)

- Is duplicate of Bug #18061: Execshield test: libruby.so.N.N.N: FAIL: property-note test because no .note.gnu.property section found added

#4 - 06/06/2024 07:53 PM - alanwu (Alan Wu)

- Status changed from Open to Closed

Closing as duplicate as suggested.