Buffer overrun in util.c: ruby_hdtoa / nrv_alloc

08/16/2010 01:38 PM - pweldon (Peter Weldon)

Status: Closed
Priority: Normal
Assignee:
Target version: 2.0.0
Backport:
ruby -v: ruby 1.9.3dev (2010-08-15)
[i386-mswin32_100]

Description
BEGIN
util.c (ruby_hdtoa) causes buffer overrun in nrv_alloc when returning copies of constant strings ("0", "NaN", "Infinity"). Detected while running ruby 1.9.3dev (2010-08-15) [i386-mswin32_100], linked with debug crt libs, heap corruption is detected while running test/ruby/test_sprintf.rb.

Patch attached:
- consistently handling of const return strings in ruby_hdtoa, ruby_dtoa, using rv_strdup
- avoid strlen in rv_strdup
- remove handrolled memcpy in nrv_alloc
END

History
#1 - 08/16/2010 07:27 PM - nobu (Nobuyoshi Nakada)
- Status changed from Open to Closed
- % Done changed from 0 to 100

BEGIN
This issue was solved with changeset r29010.
Peter, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.
END

Files
- i386-mswin32_100.txt 5.73 KB 08/16/2010 pweldon (Peter Weldon)
- util.c.patch 2.16 KB 08/16/2010 pweldon (Peter Weldon)