Docker's latest version of privilege escalation vulnerability

六月 26, 2020

0x00 Vulnerability analysis

1.com.docker.vmnetd is a launch service that runs at root authority; communicates with the client (Docker) through a local socket; after analysis, it is found that the client is not verified during the communication process, resulting in the risk of elevated permissions

<

2. The two main functions in main_handle are vmnet_handshake_Perform and vmnetd_commands_Handle; vmnet_handshake_Perform function mainly initializes the message and obtains the corresponding client command. vmnetd_commands_Handle function calls the corresponding callback function according to the obtained command.

```
| If | [ universal limit(__inst. | _omet. ') [_inst. | _inst. | _i
```

2.1 vmnet_handshake_Perform

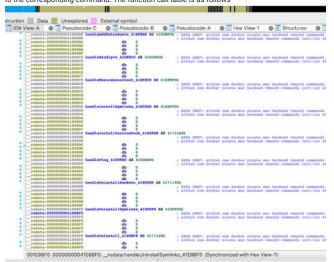
2.1.1 First obtain the initialization message (3 packets) requested by the client through vmnet_handshake_readInitMessage. The message structure is as follows

2.1.2 Then call vmnet_handshake_writeInitMessage to respond to the client's request and call vmnet_handshake_readCommand to get the client's requested command (the message is 1 byte in size)

```
| The content of the
```

2.2 vmnetd_commands_Handle

2.2.1 vmnetd_commands_Handle will call the corresponding callback function (vmnetd_commands_handlers) according to the corresponding command. The function call table is as follows



2.2.2 The vmnetd_commands_handlers callback function will be initialized in the vmnetd_commands_init function

according to the corresponding command



2.3 vmnetd_commands_handleInstallSymlinks

2.3.1 After the function obtains the message requested by the client (installation path information), set the corresponding symbolic link in the /usr/local/bin/ directory to point to the corresponding binary program; later set the file permissions through vmnetd_commands_doSymlink

0x01 Exploit

1.Create a test file in the /var/log directory

2. After compiling and running poc_docker, test file permissions will be modified

< 漏洞分析 漏洞挖掘

_____ TravisC 2020年9月13日00:34

Hi! University student here. Me and my friends are writing a report on this cve, was wondering if you could share the poc_docker.c file with us? It would be a great help!

回复

panindia 2021年2月18日21:09

ngo foundation in india

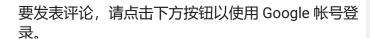
Plan india is a child rights organisation providing children, especially girls, with access to education, healthcare, protection and livelihood opportunities. • Plan India is a child rights organization providing children, especially girls, with access to education, healthcare, protection and livelihood opportunities

回复

Unow22 2021年10月12日 08:21

The great part about this method is that you can do it from the comfort of your own home, with the only cost being the materials you'll need. The Jerry G Method The Jerry G method is a way of removing drug traces from your hair. In an old marijuana forum, a popular cannabis user who went by the handle Jerry G invented the approach in 2008. Pros • Contains natural urine compounds • Perfect pH balance and consistency • Very easy to use • Has a built-in heat source Cons • Pricier than other brands • Short shelf life Hey, drug tests are no joke, so it's only right that you take it as seriously as you can. And if you regularly hit the pipe, then you know a simple cleanse won't do, especially if it's one of those dreaded surprise drug tests you're talking about. Worry not, my skeevy stoner friend, because you can always use the Clear Choice Incognito Belt synthetic urine kit: it's perhaps the absolute best fake pee you can get in the market right now, and rightfully so.

回复





此博客中的热门博文

Opencart-v3-0-3-0 user changes password at csrf vulnerability

六月28,2018



Software Link: https://github.com/opencart/opencart/ Date: 06.28.2018 Exploit Author:CK01 Version:<= V3-0-3-0 0x00 Vulnerability analysis The user token was not verified at the password change, causing the csrf vulnerability to modify the user password ...

阅读全文

Charles 4.2.7 XML External Entity

十一月 12, 2018



Software Link: https://www.charlesproxy.com Date:11.12.2018 Exploit Author:CK01 Version:<=4.2.7 Security Issue: The XML External Entity vulnerability exists in the Charles import/export setup option. If the user imports the "Charles Settings.xml" of the attacker, the internal network may be de

阅读全文

B 由 Blogger 提供支持

主题背景图片创建者: Michael Elkan

