New issue

Jump to bottom

# Remote code execution vulnerability #238

Closed **deenrookie** opened this issue on Jun 1, 2020 · 1 comment

**deenrookie** commented on Jun 1, 2020

Hi, this is Tencent **Xcheck** team. Our code safety check tool Xcheck has found several unserialize vulnerabilities in this project（v4, v5, v6）. It leads to remote code execution. Here are the details.

**v6**

1. app/admin/controller/api/Update.php
   line: 46 `$this->rules = unserialize($this->request->post('rules', 'a:0:{}', ''));`
   line: 47 `$this->ignore = unserialize($this->request->post('ignore', 'a:0:{}', ''));`

**v6 v5 v4**
2. app/wechat/controller/api/Push.php
line: 102 `$this->receive = $this->toLower(unserialize($this->request->post('receive', '', null)));`

Prevent from abusing of this vulnerability, we don't provide proof of concept. We hope to repair it as soon as possible.

**From Xcheck Team**

**zoujingli** added a commit that referenced this issue on Jun 15, 2020

#238 Testing 6ccd405

**zoujingli** added a commit that referenced this issue on Jun 16, 2020

#238 Data format transfer changed 640a61a

**zoujingli** added a commit that referenced this issue on Jun 16, 2020

#238 修改回复参数 b8a2ded

**zoujingli** commented on Jun 16, 2020 Owner

ThinkAdmin V6 接口的序列化数据全部改成了 JSON
更新方式：
composer update 更新 vendor 中的 think-library
php think xadmin:install admin 更新 admin 模块
php think xadmin:install wechat 更新 wechat 模块

**zoujingli** closed this as completed on Jun 16, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants