三代WAF是否涉及CVE-2022-31625 CVE-2022-31626

漏洞相关 **孔梦龙** 2022-06-20 发表

漏洞相关信息

漏洞编号： CVE-2022-31625 CVE-2022-31626
漏洞名称： PHP远程代码执行漏洞（CVE-2022-31625 CVE-2022-31626）
产品型号及版本： 三代WAF

漏洞描述

近日，WebRAY安全服务产品线监测到PHP 官方发布了关于PHP存在远程代码执行漏洞的漏洞通告，漏洞编号分别为：CVE-2022-31625、CVE-2022-31626。其中CVE-2022-31625是由于PHP_FUNCTION中分配在堆上的数组清除不及时，导致错误的再次调用php_pgsql_free_params()函数时，可能会使用之前未及时清除的数组值，从而造成远程代码执行；CVE-2022-31626则是由于PHP的mysqlnd拓展中存在堆缓冲区溢出漏洞，拥有php数据库的连接权限并建立恶意MySQL服务器的攻击者，通过诱导主机以mysqlnd主动连接该服务器从而触发缓冲区溢出漏洞，最终实现远程代码执行，像是Adminer、 PHPmyAdmin这类基于php的数据库管理软件均可能受该漏洞影响。由于漏洞危害较大，WebRAY安全服务产品线建议相关用户做好防护并及时做好版本升级工作。
PHP是一个拥有众多开发者的开源软件项目，也是一种在服务器端执行的脚本语言，尤其适用于Web开发并可嵌入HTML中。PHP同时支持面向对象和面向过程的开发，使用上非常灵活。
WebRAY安全服务产品线也将持续关注该漏洞进展，并及时为您更新该漏洞信息。

漏洞解决方案

不涉及