# 云数产品是否涉及PHP 内存释放后重用漏洞、缓冲区溢出漏洞

程鑫 2022-06-15 发表

## 漏洞相关信息

漏洞编号： CVE-2022-31625、CVE-2022-31626

漏洞名称： PHP 内存释放后重用漏洞、缓冲区溢出漏洞

产品型号及版本： CAS&UIS&VDI&ONEStor&CloudOS&大数据&数据库

## 漏洞描述

PHP（Hypertext Preprocessor），是一种被广泛用于开发 Web 项目的服务 端通用脚本语言，于 1995 年发布 1.0 版本，目前最新版本为 8.1.7。 北京时间 2022 年 6 月 10 日，PHP 发布了 PHP 7.4.30 和 8.1.7 版本，并披露 修复了 2 个高危漏洞。内存释放后重用漏洞，在 pg_query_params 函数中，用于 存储查询参数的 char* 数组未初始化，来自先前请求的延迟值可以被释放，最 终导致远程代码执行；在 php_mysqlnd_change_auth_response_write 函数中， 将用户提交的密码复制到缓冲区时，由于未校验加上 MYSQLND_HEADER_SIZE 的长 度，将发生缓冲区溢出导致远程代码执行，攻击者可以通过架设恶意数据库服务 器来攻击 Adminer、PHPmyAdmin 等 DBMS 工具。 暂未监测到上述漏洞在野利用，POC 已公开，漏洞详情已知。

影响范围：

PHP5 <= 5.6.40

PHP7 < 7.4.30

PHP8 < 8.1.7 || < 8.0.20

安全版本：

PHP5 的维护更新已于 2018 年 12 月 31 日终止

PHP7 >= 7.4.30

PHP8 >= 8.1.7 || >= 8.0.20

## 漏洞解决方案

云数产品不涉及，未使用该语言。