

PHP 远程代码执行漏洞 (CVE-2026-109618 和 CVE-2026-109619) 缓解方案

2026 年 10 月

目 录

1 概述.....	3
2 项目描述.....	3
3 漏洞缓解步骤.....	3

1 概述

撰写此文的主要目的是为了指导云科容翼设备针对 CVE-2026-109618 和 CVE-2026-109619 漏洞缓解措施。在实际工作实施工作前，将所有实施步骤、方法和各方需完成的任务明确。

2 项目描述

PHP 远程代码执行漏洞，特定条件下允许攻击者远程执行代码 受影响版本：
云科容翼/威翼 YK-ADC 17.1-17.5 的所有版本（包含低于 V17 版本） 影响范围：控制平面

漏洞级别：High/7.5 (CVSS v3.1)

3 漏洞缓解步骤

漏洞规避措施，针对 php 设置特定的参数可以规避此漏洞： 在设备上创建新文件/etc/php.ini.d/K000163821.ini，并写入如下内容：

The configuration mitigations recommended by PHP for CVE-2026-109618 and CVE-2026-109619

; These will NOT survive an upgrade of YK-ADC.

memory_limit = -1

post_max_size = 8M

upload_max_filesize = 7M

session.upload_progress.enabled = 0

输入完毕，执行:wq!保存配置

再执行tmsh restart sys service httpd，让上述参数生效。

验证设备是否可以通过图形化界面登录

如有需要，可以在/var/tmp/下创建 check.php

vim /var/tmp/check.php，然后输入 i 允许插入内容：

```
<?php
```

```
echo "memory_limit: ".ini_get('memory_limit')."\n";
```

```
echo "post_max_size: ".ini_get('post_max_size')."\n";
```

```
echo "upload_max_filesize: ".ini_get('upload_max_filesize')."\n";
```

```
echo "session.upload_progress.enabled:
```

```
".ini_get('session.upload_progress.enabled')."\n";
```

```
?>
```

输入完毕，执行:wq!保存配置

php /var/tmp/check.php 查看参数，确认修改成功

```
post_max_size = 8M
```

```
upload_max_filesize = 7M
```

```
session.upload_progress.enabled = 0
```

重启 httpd 进程使配置生效，重启 httpd 进程不影响业务，只会短暂影响登陆界面

```
bigstart restart httpdi
```

i

系统回退	系统回退，涉及设备如下 主机 备机	主机、备机删除/etc/php.ini.d/ cd /etc/php.ini.d/ rm -rf K000163821.ini tmsh restart sys service httpd php /var/tmp/check.php 查看参数，确认回退成功
------	-------------------------	---