山西省互联网网络安全预警信息通报

山西省通信管理局
主办：国家计算机网络应急技术处理协调中心山西分中心　2021 年 4 月 23 日

关于亿邮电子邮件系统存在远程命令执行漏洞的安全公告

近日，国家信息安全漏洞共享平台（CNVD）收录了亿邮电子邮件系统远程命令执行漏洞（CNVD-2021-26422）。攻击者利用该漏洞，可在未授权的情况实现远程命令执行，获取目标服务器权限。目前，漏洞利用细节已公开，厂商已于 4 月 9 日发布版本补丁完成修复。

一、漏洞情况分析

亿邮电子邮件系统是由北京亿中邮信息技术有限公司（以下简称亿邮公司）开发的一款面向中大型集团企业、政府、高校用户的国产邮件系统。亿邮电子邮件系统采用了自主研发 MTA 引擎、分布式文件系统存储方式、多对列机制、ECS 存储子系统、Cache 系统等多项核心技术，提供了丰富的邮件功能。

近日，有安全人员披露了亿邮电子邮件系统高危漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意请求，使用 POST 方法在目标服务器执行命令，获取目标服务器权限，控制目标服务器。目前，漏洞细节已公开，厂商已发布版本补丁完成修复。

CNVD 对该漏洞的综合评级为“高危”。

二、漏洞影响范围

漏洞影响的产品版本为亿邮电子邮件系统 V8.3-V8.13 的部分二次开发版本。

亿邮电子邮件系统信创版本及 V8.13 以后版本不受影响。

三、处置措施

目前，亿邮公司已通过技术支持渠道向用户提供了补丁程序。

CNVD 建议使用亿邮电子邮件系统的用户按照如下方式进行自查，发现存在漏洞后，及时联系亿邮公司进行漏洞修补。

在邮件系统服务器上执行如下命令:

ls /usr/local/eyou/mail/lib/php/monitor (8.10.x 及以后版本)

ls /usr/local/eyou/mail/app/lib/php/monitor (8.10.x 及以前版本)

*如不了解具体版本号，上述两条命令可不分版本都执行一下

如所有的验证命令都返回“No such file or directory”或“没有那个文件或目录”则证明不存在漏洞，反之则漏洞存在。

使用涉及版本的用户可通过400服务电话（400-111-6088）联系亿邮公司售后服务，亿邮公司售后维护人员可提供补丁包安装咨询、远程技术支持以及上门服务。