

# 知 iMC&U-Center不涉及漏洞 NIUSHOP开源商城系统 (V2.3) 存在任意文件上传漏洞

PLAT 付帅文 2021-04-18 发表

## 漏洞相关信息

漏洞编号: 无

漏洞名称: NIUSHOP开源商城系统 (V2.3) 存在任意文件上传漏洞

产品型号及版本: iMC\_1.0系列产品, U-Center1.0系列产品

## 漏洞描述

漏洞原理: NIUSHOP系统的商品规格图片上传处仅对文件的MIME做了检测, 未对上传文件进行后缀名的检测及重命名, 攻击者可以绕过上传控制; 且该上传点对文件做检测后处理不完善, 未对检测不通过的文件进行删除或相应处理, 对上传文件的重命名处理过于简单, 可通过爆破猜出重命名的文件名并进行访问利用。 处置/应对措施: 对上传目录中已上传的PHP文件进行删除处理; 增加上传点的文件后缀名检查及重命名; 更改文件重命名规则; 将检查不通过的上传文件移至不可访问目录, 不再保存于WEB服务目录中。

## 漏洞解决方案

iMC&U-Center1.0系列皆不涉及该漏洞，可参考漏洞报告进行漏洞修复，不影响iMC&U-Center1.0功能

•

