泛微 E-Office 任意文件上传漏洞

CVE-2023-2648

2023 年 5 月 12 日

一、漏洞概要

漏洞名称	泛微 E-Office 任意文件上传漏洞(CVE-2023-2648)
发布时间	2023 年 5 月 12 日
组件名称	泛微 E-Office
影响范围	泛微 E-Office 9.5
漏洞类型	任意文件上传
利用条件	1、用户认证：未知 2、前置条件：未知 3、触发方式：远程
综合评价	<综合评定利用难度>：未知 <综合评定威胁等级>:高危,能造成远程代码执行。
官方解决方案	已发布

二、漏洞分析

2.1 组件介绍

泛微 E-Office 软件拥有行政审批，人事管理，信息沟通，业务管控，工作执行等等功能服务，可以助力更高效移动协同工作。

2.2 漏洞描述

2023 年 5 月 12 日，深信服安全团队监测到一则泛微 E-Office 组件存在任意文件上传漏洞的信息，漏洞编号：CVE-2023-2648，漏洞威胁等级：高危。

该漏洞是由于/inc/jquery/uploadify/uploadify.php 的参数的限制存在错误，攻击者可利用该漏洞，构造恶意数据执行任意文件上传攻击，最终获取服务器最高权限。

三、影响范围

泛微 E-Office 是较为流行的自动化企业管理软件之一，可能受漏洞影响的资产主要位于国内各地。

目前受影响的泛微 E-Office 版本：

泛微 E-Office 9.5

四、解决方案

4.1 修复建议

1.官方修复建议

目前厂商暂未发布修复措施解决此安全问题，建议随时关注厂商主页或联系厂商以获取解决办法：

https://www.e-office.cn/

5.2 深信服解决方案

1.风险资产发现

支持对 泛微 E-Office 9.5 的主动检测，可**批量检出**业务场景中该事件的**受影响资产**情况，相关产品如下：

【深信服主机安全检测响应平台 CWPP】已发布资产检测方案。

【深信服云镜 YJ】已发布资产检测方案。

五、时间轴

2023/5/12　深信服监测到泛微 E-Office 任意文件上传漏洞(CVE-2023-2648)攻击信息。

2023/5/12　深信服千里目安全技术中心发布漏洞通告。

六、参考链接

https://www.e-office.cn/

七、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。