关于 Foxmail 邮件客户端存在跨站脚本攻击漏洞的安全公告

2025-04-10 16:00:56

安全公告编号:CNTA-2025-0007

2025 年 3 月 20 日，国家信息安全漏洞共享平台（CNVD）收录了 Foxmail 邮件客户端跨站脚本攻击漏洞（CNVD-2025-06036）。攻击者利用该漏洞作为攻击入口，向目标用户对象发送包含恶意代码的电子邮件，用户仅浏览邮件即被植入木马，其主机终端即被控。目前，该漏洞已发现被利用进行攻击，厂商已发布新版本完成漏洞修复，CNVD 建议受影响的单位和用户立即升级至最新版本。

一、漏洞情况分析

Foxmail 是我国知名电子邮件客户端之一，其上市时间自 1997 年第一版公测开始至今已 28 年，Foxmail 电子邮件客户端在 2005 年 3 月 16 日被腾讯公司收购，由腾讯公司运行维护。

2025 年 3 月 20 日，国家信息安全漏洞共享平台（CNVD）收录了 Foxmail 邮件客户端跨站脚本攻击漏洞。由于 Foxmail 在处理加载邮件正文时，对危险内容的过滤处理逻辑存在缺陷，攻击者构造包含恶意指令代码的电子邮件向目标用户发送，目标用户仅需使用 Foxmail 打开恶意邮件，无需其他点击操作，恶意指令代码即可被用户主机加载执行，具有较高的攻击隐蔽性。攻击者继而利用其他漏洞，在未授权的前提下实现对目标主机的木马文件本地写入和控制权限获取。

CNVD 对该漏洞的综合评级为“中危”。

二、漏洞影响范围

漏洞影响的产品和版本：

Foxmail < 7.2.25

三、漏洞处置建议

3 月 28 日，腾讯公司已紧急发布新版本修复该漏洞，CNVD 建议受影响的单位和用户立即将 Foxmail 升级至最新版本：

https://www.foxmail.com/

攻击者通常使用社会工程学等手段，对恶意邮件的标题、内容及附件进行伪装，诱骗用户点击访问，CNVD 建议用户做好安全防范措施，不要打开来历不明的邮件。