CVE-2023-27363

福昕Foxit PDF

远程代码执行漏洞

目录

[1. 漏洞描述 3](#_Toc27475)

[2. 影响版本 3](#_Toc25949)

[3. 环境部署 3](#_Toc5232)

[4. 漏洞复现 9](#_Toc11219)

# 漏洞描述

漏洞概述福建福昕软件开发股份有限公司是一家国际化运营的PDF电子文档解决方案提供厂商，提供文档的生成、转换、显示、编辑、搜索、打印、存储、签章、表单、保护、安全分发管理等涵盖文档生命周期的产品技术与解决方案。其下产品Foxit PDF Reader和Foxit PDF Editor的javascript函数exportXFAData，只验证了cPath参数中文件夹路径是否存在，未校验文件后缀的合法性，导致可以将交互式表单(XML Forms Architecture，简称XFA)数据导出为任意后缀的文件。XFA数据中可以包含javascript代码，将其导出为后缀为hta的文件，写入Windows Startup 文件夹，该文件可以在计算机重启后自动运行，实现任意代码执行。

# 影响版本

Foxit PDF Reader <= 12.1.1.15289

Foxit PDF Editor 12.x <= 12.1.1.15289

Foxit PDF Editor 11.x <= 11.2.5.53785

Foxit PDF Editor <= 10.1.11.37866

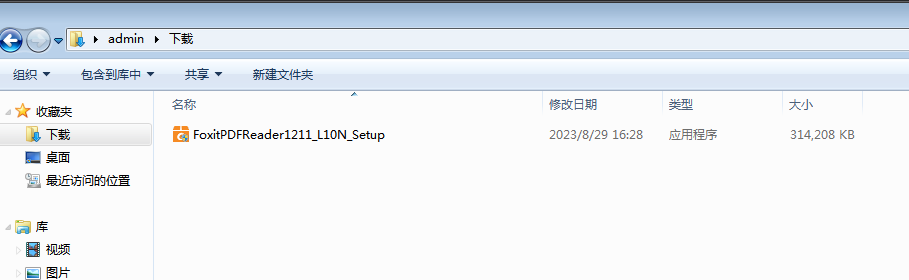
# 环境部署

靶机：Windows 7，ip：172.16.5.182

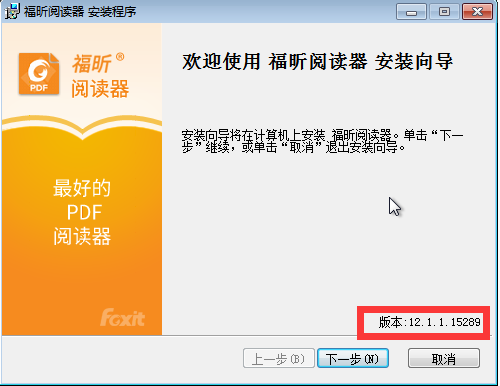
渗透机：Windows 7，ip：172.16.5.182

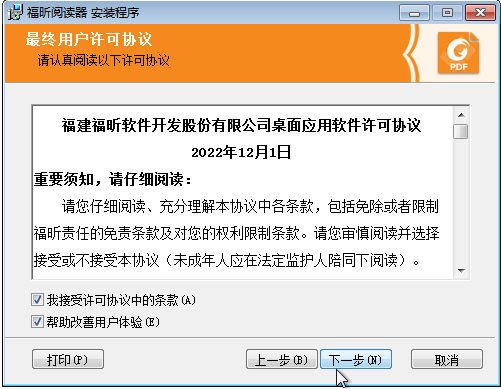
下载含有漏洞的软件

<https://cdn01.foxitsoftware.com/product/reader/desktop/win/12.1.1/FoxitPDFReader1211_L10N_Setup.exe>



安装





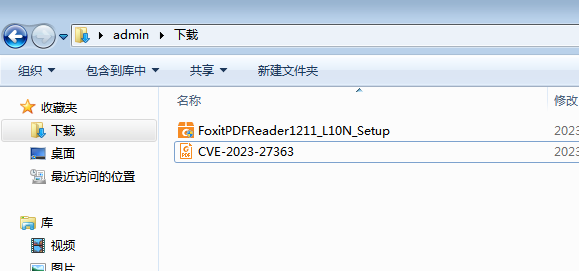


# 漏洞复现

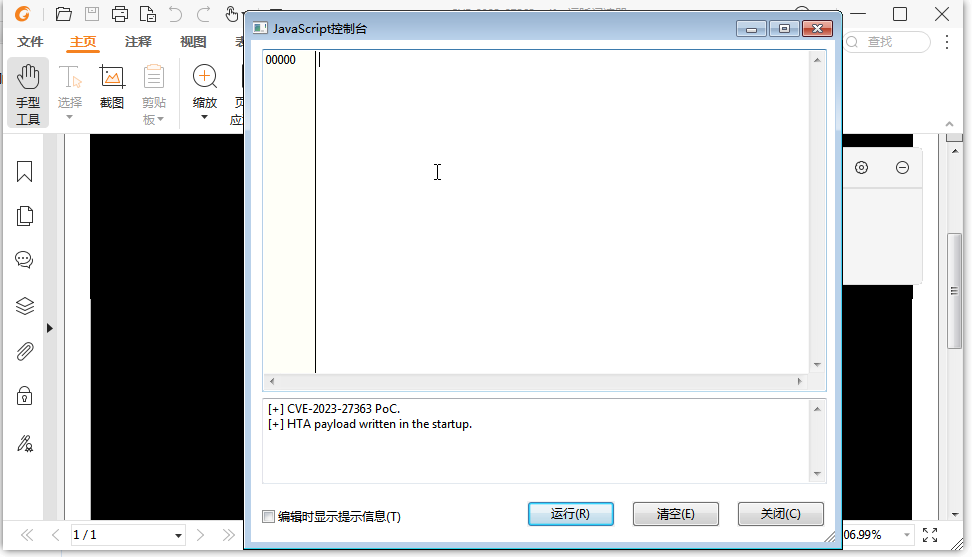
**【步骤一】**

**下载含有而已代码的pdf文件**

<https://github.com/webraybtl/CVE-2023-27363/blob/main/CVE-2023-27363.pdf>

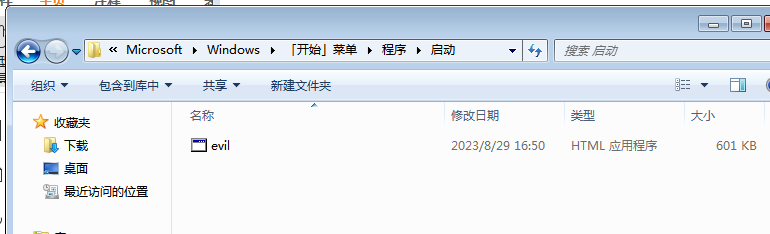


**【步骤二】使用Foxit打开该pdf**

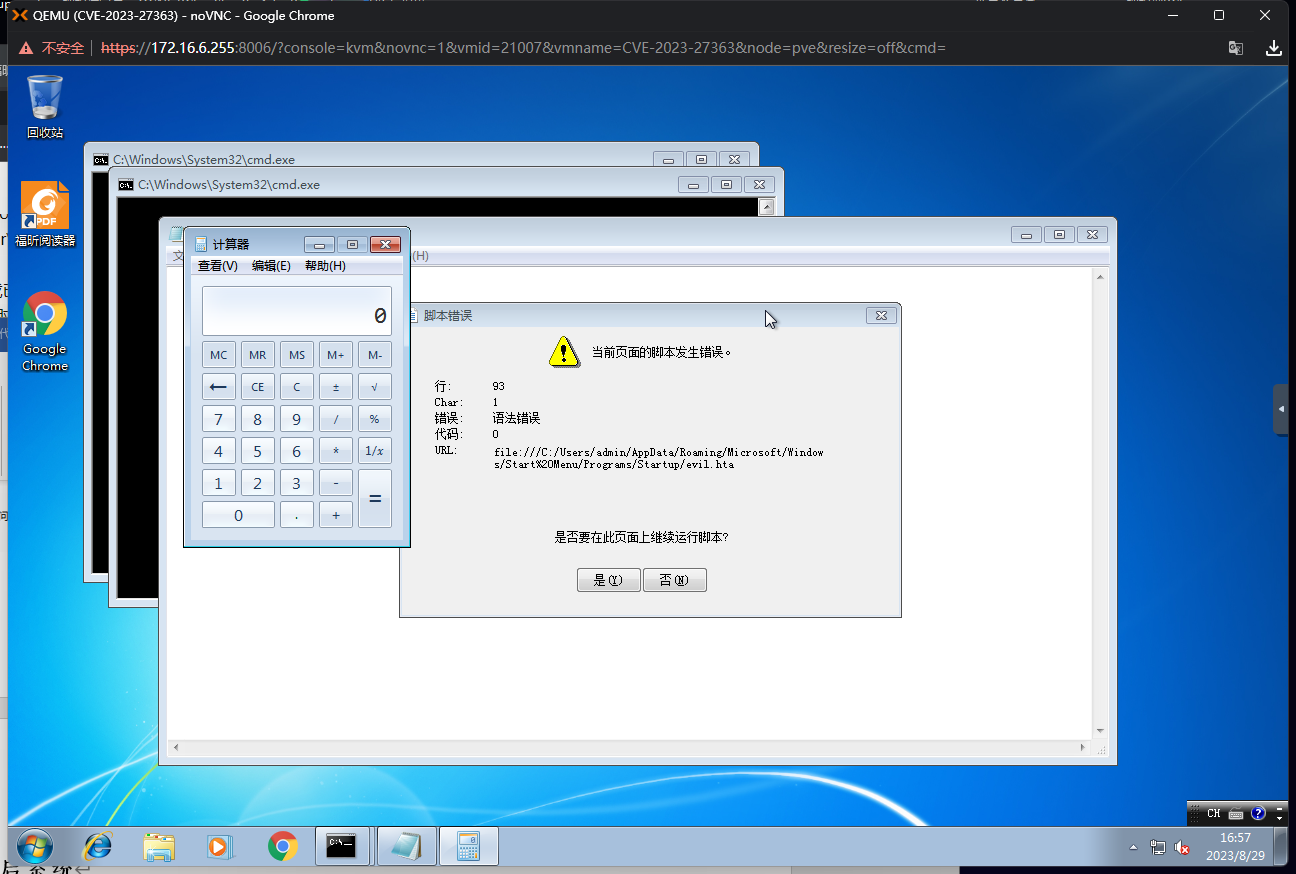


**发现其打开了JavaScript控制台并且将代码程序写入了开机自启动菜单**

**打开自启动菜单**



**【步骤三】重启系统**



**开机发现计算器和记事本自启动，恶意命令执行成功**

