Microsoft Office 远程代码执行漏洞通告

2021 年 4 月 23 日

目录

一、 漏洞概要

漏洞名称	Microsoft Office 远程代码执行漏洞
影响组件	Microsoft Office
影响范围	MicrosoftOffice2013ServicePack1(32/64-biteditions) MicrosoftOffice2013RTServicePack1 MicrosoftOffice2010ServicePack2(32/64-biteditions) MicrosoftOffice2016(32/64-bitedition)
漏洞类型	远程代码执行
利用条件	1、用户认证：否 2、前置条件：需打开恶意文档 3、触发方式：远程
综合评价	<综合评定利用难度>：困难，需要高权限用户执行恶意程序。 <综合评定威胁等级>：高危，能造成远程代码执行。

二、 漏洞分析

2.1 组件介绍

Microsoft Office 是由 Microsoft(微软)公司开发的一套基于 Windows 操作系统的办公软件套装。常用组件有 Word、Excel、PowerPoint 等。

2.2 漏洞描述

2021 年 4 月 22 日，深信服安全团队监测到微软官方发布了一则安全通告，披露了 Office 组件存在远程代码执行漏洞，漏洞编号：CVE-2021-27059，漏洞危害：中危。受害者打开攻击者精心构造的恶意文档触发该漏洞，攻击者即可利用该漏洞远程执行代码。

三、 影响范围

MicrosoftOffice 可以运行在所有 Windows 平台上，由于其便捷性和安全性被广泛使用，成为最流行的办公软件套件之一。全球有大量使用 Office 的用户。

目前受影响的 MicrosoftOffice 版本：

MicrosoftOffice2013ServicePack1(32/64-biteditions)

MicrosoftOffice2013RTServicePack1

MicrosoftOffice2010ServicePack2(32/64-biteditions)

MicrosoftOffice2016(32/64-bitedition)

四、 解决方案

4.1、 官方解决方案

当前官方已发布受影响版本的对应补丁，建议受影响的用户及时更新官方的安全补丁。链接如下：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27059

4.2、 如何检测组件系统版本

在 Office 界面设置中点击版本即可。