

Internet Explorer 远程代码执行 漏洞通告

2021 年 4 月 23 日

目录

一、	漏洞概要.....	3
二、	漏洞分析.....	4
三、	影响范围.....	5
四、	解决方案.....	6

一、漏洞概要

漏洞名称	Internet Explorer 远程代码执行漏洞
影响组件	Internet Explorer
影响范围	IE11: WindowsServer2019 Windows10Version20H2forx64-basedSystems Windows10Version2004forx64-based/ARM64-basedSystems Windows10Version1909for32-bit/x64/ARM64-basedSystems Windows10Version1809forARM64-basedSystems Windows10Version1809for32-bit/x64-basedSystems Windows10Version1803for32-bit/x64-basedSystems Windows10Version20H2for32-bit/ARM64-basedSystems
漏洞类型	远程代码执行
利用条件	用户认证：不需要用户认证 触发方式：远程
综合评价	<综合评定利用难度>：容易，无需授权即可远程代码执行。 <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

Internet Explorer (旧称 Microsoft Internet Explorer 和 Windows Internet Explorer, 简称 IE 或 MSIE), 是微软所开发的图形用户界面网页浏览器。自从 1995 年开始, 内置在各个新版本的 Windows 操作系统, 是微软 Windows 操作系统的一个组成部分。

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 Internet Explorer 组件存在远程代码执行漏洞, 漏洞编号: CVE-2021-27085, 漏洞危害: 高危。受害者打开攻击者构造的恶意网站即可触发该漏洞, 攻击者可利用该漏洞造成远程代码执行。

三、影响范围

IE 可以运行在所有 Windows 计算机平台上，由于其安全性被广泛使用，成为非常流行的浏览器软件之一。

目前受影响的 IE 版本：

运行 IE11 的以下平台：

WindowsServer2019

Windows10Version20H2forx64-basedSystems

Windows10Version2004forx64-based/ARM64-basedSystems

Windows10Version1909for32-bit/x64/ARM64-basedSystems

Windows10Version1809forARM64-basedSystems

Windows10Version1809for32-bit/x64-basedSystems

Windows10Version1803for32-bit/x64-basedSystems

Windows10Version20H2for32-bit/ARM64-basedSystems

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/vulnerability/CVE-2021-27085>

4.2、 如何检测组件系统版本

在 C:\ProgramFiles\InternetExplorer 目录下找到 iexplore.exe 选中后右键找到属性-详细信息即可找到对应版本。

