**关于Win7系统停服IE远程执行漏洞利用**

**安全防护说明**

# 一、Win7系统停服背景

2020年1月14日，微软正式宣告Windows 7系统停止更新，官方停止技术支持、软件更新和安全问题的修复，数以亿计仍在运行Windows 7系统的计算机失去了保护屏障，面临重大安全威胁。



截止到2019年10月底，国内Windows7系统市场份额占比仍有近6成，Windows 7的终结，意味着庞大的用户失去了微软官方的所有支持，包括软件更新、补丁修复和防火墙保障，将直面各类利用漏洞等威胁进行的攻击。

2020年1月，360安全大脑在全球范围内率先监测到一起利用IE浏览器脚本引擎0day漏洞的APT攻击。利用该漏洞，攻击者可诱使用户访问恶意网页，触发该漏洞后可以直接获得对用户系统的控制，无论IE浏览器还是火狐浏览器打开都会中招。用户在毫无防备的情况下，可被植入勒索病毒，甚至被黑客监听监控，执行窃取敏感信息等任意操作。360安全大脑就全球首家捕捉到此次攻击，并将其命名为“双星”0day漏洞攻击。

# 二、提醒用户注意事项

针对Win7系统停服时期爆发出的“双星”漏洞攻击事件，360安全大脑特别提醒广大用户，请勿随意打开未知网站。尤其是Windows 7系统用户，应及时做好准备、全力应对系统停服后带来的安全问题，可通过360Win7盾甲提升电脑安全性。同时，提醒各相关企、事业单位，警惕利用“双星”漏洞发动的定向攻击，密切跟踪该漏洞的最新情况，及时使用安全软件防御可能的漏洞攻击。360安全大脑将对“双星”漏洞持续跟进关注，并推进相关安全补丁的发布。



# 三、应急措施

建议：限制对JScript.dll的访问，可暂时规避该安全风险，但可能导致网站无法正常浏览。
对于32位系统，在管理命令提示符处输入以下命令：

takeown /f %windir%\\system32\\jscript\.dll

cacls %windir%\\system32\\jscript\.dll /E /P everyone:N

对于64位系统，在管理命令提示符处输入以下命令：

takeown /f %windir%\\syswow64\\jscript\.dll

cacls %windir%\\syswow64\\jscript\.dll /E /P everyone:N

 takeown /f %windir%\\system32\\jscript\.dll

cacls %windir%\\system32\\jscript\.dll /E /P everyone:N

实施这些步骤可能会导致依赖jscript.dll的组件功能减少。为了得到完全保护，建议尽快安装此更新。在安装更新之前，请还原缓解步骤以返回到完整状态。

**如何撤消临时措施**

**对于32位系统，在管理命令提示符处输入以下命令：**

cacls %windir%\\system32\\jscript\.dll /E /R everyone

**对于64位系统，在管理命令提示符处输入以下命令：**

cacls %windir%\\system32\\jscript\.dll /E /R everyone

cacls %windir%\\syswow64\\jscript\.dll /E /R everyone

# 四、技术支持

可下载安装360安全大脑Windows 7盾甲企业版（目前可免费使用）加强防护。

**Windows 7盾甲企业版下载地址：**

https://yunpan.360.cn/surl\_yrW9fAQSpeR (提取码：9991)

详细的安装文档参照附件《Windows7盾甲企业版部署指南》

该版本一键管理全网终端，支持Windows全平台已知漏洞的补丁修复，结合针对漏洞威胁全新推出的360微补丁功能，在面对“双星”0day漏洞等突发性高危漏洞时，360微补丁可通过先行自动覆盖漏洞，解决防护能力滞后问题，全天候守护PC安全。

# 关于微软Win7系统IE远程执行漏洞利用的相关说明<http://www.360.cn/n/11481.html>