

360 向广大政企用户发出 Win7 漏洞威胁预警通告 | 极客公园

Archived: 2026-04-05 21:18:51 UTC

2020 年 1 月 14 日，Win7 正式宣告停服，自此微软官方将不再对 Win7 系统进行任何问题的技术支持、软件更新，以及安全更新或修复。在此之际，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。

据 360 安全专家解读，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，产生的影响不亚于此前 WannaCry 勒索病毒带来的伤害。此漏洞波及范围不仅影响所有微软用户，政府、企业用户更将成为首要攻击目标。

针对此问题，360 独家推出 360 安全大脑 Windows 7 盾甲企业版，支持 Windows 全平台已知漏洞的补丁修复，针对突发性高位漏洞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。360 建议广大政府、企业 Win7 系统用户联系 360 安全团队获取帮助，以抵御新型 IE 浏览器 0day 漏洞威胁，并于 1 月 15 日官方发布《360 安全大脑关于微软 Win7 系统 IE 远程执行漏洞利用的告客户书》，原文如下：

(一) 通告背景

2020 年 1 月，360 安全大脑在 Win7 停服之际，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。在捕获到该 IE 浏览器 0day 漏洞攻击的第一时间，360 安全大脑对漏洞利用背后的 APT 组织进行追踪与溯源分析。目前，从已捕获攻击细节及特征初步判定，此次 IE 浏览器 0day 漏洞攻击疑似出自半岛的 APT 组织 Darkhotel(APT-C-06) 之手。Darkhotel(APT-C-06) 是一个活跃近十余年的东亚背景 APT 组织，相关攻击行动最早可以追溯到 2007 年，而此次截获的 IE 浏览器 0day 漏洞攻击，也并非 360 安全大脑第一捕获该组织动向。

2018 年 4 月，360 安全大脑就曾在全球范围内，率先监控到了该组织使用 0day 漏洞进行 APT 攻击。而从 360 安全大脑溯源分析报告来看，该 APT 组织长期目标涉及中、俄、日等国政府及组织机构或企业单位，尤其针对中国重点省份外贸企业单位和相关机构展开攻击，更是由来已久。在捕获到该 IE 浏览器 0day 漏洞后，360 安全团队已第一时间向微软官方提交了详细漏洞报告，目前微软官方已经在跟进。但是，必须一提的是，由于 2020 年 1 月 14 日起，Win7 正式宣告停服，微软官方将不再对 Win7 系统进行任何问题的技术支持、软件更新，以及安全更新或修复，这意味着该 IE 浏览器 0day 漏洞修复补丁将不再覆盖 Win7 系统，换言之，所有 Win7 用户将悉数暴露在该漏洞的阴霾之下。对此，360 安全团队建议广大用户及时更新软件补丁，Win7 系统用户则尽快下载安装 360 安全大脑 Windows 7 盾甲企业版抵御新型 IE 浏览器 0day 漏洞威胁。

(二) 文档信息

关键字	微软 IE JScript RCE 远程命令执行
-----	--------------------------

发布日期	2020 年 01 月 14 日
更新日期	2020 年 01 月 14 日
TLP	WHITE
分析团队	360 核心安全事业部高级威胁应对团队

(三) 漏洞概要

漏洞名称	微软 IE 脚本引擎远程代码执行漏洞
威胁类型	远程代码执行
威胁等级	严重
漏洞发现者	360 安全大脑
利用场景	攻击者可能会通过欺骗未修补的 IE 版本的用户访问恶意制作的网页，触发内存损坏漏洞获取任意代码执行从而控制用户系统。
受影响系统及应用版本	影响下列 windows 操作系统 Internet Explorer 11 版本 Windows 10 Windows 8.1 Windows 7 Windows Server 2012/R2 Windows Server 2008 Windows Server 2016 Windows Server 2019

仅影响 Windows Server 2012 IE 10

仅影响 Windows Server 2008 SP2 IE 9

(四) 漏洞描述

该漏洞存在于 IE 中的脚本引擎 jscript.dll 中，该脚本引擎在处理内存对象的过程中，触发漏洞后会造成内存损坏，从而可以造成远程代码执行漏洞。

360 安全大脑已完整捕获攻击过程，发现攻击者的在野利用将该漏洞嵌入在 Office 文档中，用户打开 Office 文档或浏览网页都会中招。而近年来，用户量庞大、看似安全无害 Office 文档已逐渐成为 APT 攻击最青睐的载体。

一旦用户打开搭载了该漏洞的恶意文档，将会浏览恶意网页并执行攻击程序，用户甚至还未感知得到，设备就已经被控制，攻击者可趁机进行植入勒索病毒、监听监控、窃取敏感信息等任意操作。

(五) 影响面评估

根据数据显示，直至 2019 年 10 月底，国内 Windows 7 系统的市场份额占比仍有近 6 成，而对于国内而言，存在数量惊人的政府、军队、企业、个人在内的 PC 用户依然使用着 Win7 系统。

而 Windows 7 的终结，意味着数以亿计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，将直面该漏洞利用进行的攻击，并会完全暴露在安全威胁之下。

考虑到 APT 组织 Darkhotel(APT-C-06) 长期以政府组织、企业为目标的特性，IE 浏览器 0day 远程执行漏洞影响所有微软系统的特点，已经受影响版本中 Win7 系统已停服的三方面现实因素，此次 IE 浏览器 0day 漏洞波及范围不仅影响所有微软用户，政府、企业用户更将成为首要目标。

(六) 解决方案

(1) 360安全大脑 Windows 7 盾甲企业版

一面是 APT 高危漏洞攻击，一面是 Win7 系统停服，政企用户安全将何去何从？对此，广大政企用户可联系 360 公司获取 360 安全大脑 Windows 7 盾甲企业版。

联系方式如下：

联系人：刘宁

电话：(010) 52447992

(010) 5781360

邮箱：liyunpeng3@360.cn

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。

360 安全大脑作为 360 公司重磅打造的网络安全防御雷达系统，汇集超 250 亿个恶意样本，22 万亿安全日志、80 亿域名信息、2EB 以上的安全大数据，结合首创的 360QVM 人工智能引擎，实现人机协同大数据智能分析，打造预判、阻断、溯源、止损及反制多位一体的安全防御解决方案。

可查数据显示，具备大规模综合智能处置能力的 360 安全大脑，最快可在 1 天内实现漏洞补丁、免疫工具、安全策略和威胁情报推送，有效保障了 Win7 盾甲漏洞防御及修复实时性。同时，包括 Darkhotel(APT-C-06) 在内，360 安全大脑已发现 41 起针对我国发起的境外 APT 攻击，可帮助政企客户有效应对各类 APT 攻击，提升整体防御能力。Windows 7 盾甲企业版内置高级威胁发现功能，结合 360 安全大脑云端知识库，可帮助用户及时发现高级威胁攻击的踪迹，并建立全面的防御体系。

(2) 360 安全大脑-专家云 1对 1 服务

针对此次 Windows 7 停服事件相关需求，企事业单位的网络管理员可联系 360 安全大脑安服团队进行 1 对 1 服务。

座机：(010) 5244 7992

应急：yingji@360.cn

360 安全大脑 Windows 7 盾甲企业版安服人员：李云鹏 liyunpeng3@360.cn

(3) 应急措施：

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
```

Source: <http://www.geekpark.net/news/254734>