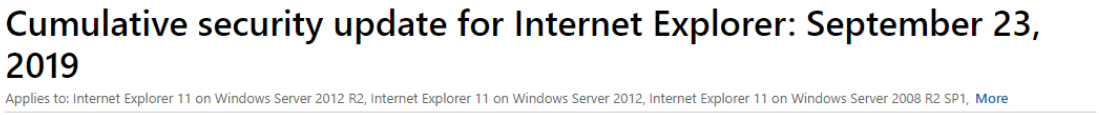
微软 IE 浏览器 JScript 脚本引擎远程代码执行漏洞通告

文档信息

编号	QiAnXinTI-SV-2019-0022
关键字	IE JScript RCE 远程命令执行 CVE-2019-1367
发布日期	2019 年 09 月 24 日
更新日期	2019 年 09 月 25 日
TLP	WHITE
分析团队	奇安信威胁情报中心红雨滴安全研究团队

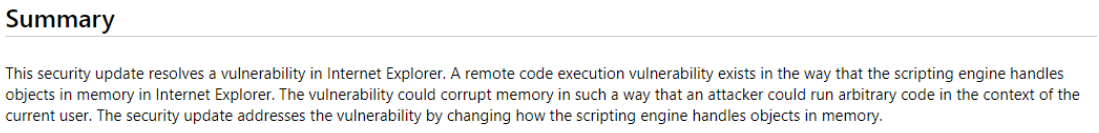
通告背景

2019 年 9 月 23 日，微软紧急官方发布安全更新，修复了一个存在于 Windows 平台的 Internet Explorer 9/10/11 版本中的远程代码执行漏洞，由 Google 威胁分析小组的安全研究员 ClémentLecigne 发现此漏洞。攻击者可能利用此漏洞通过诱使用户访问恶意网页触发漏洞从而获得对用户系统的控制。



Cumulative security update for Internet Explorer: September 23, 2019

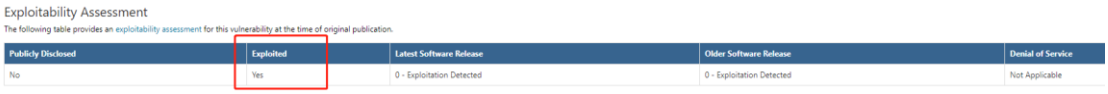
Applies to: Internet Explorer 11 on Windows Server 2012 R2, Internet Explorer 11 on Windows Server 2012, Internet Explorer 11 on Windows Server 2008 R2 SP1, More



Summary

This security update resolves a vulnerability in Internet Explorer. A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could run arbitrary code in the context of the current user. The security update addresses the vulnerability by changing how the scripting engine handles objects in memory.

从微软的描述上看，该漏洞已经存在野外利用。



Exploitability Assessment

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	Yes	0 - Exploitation Detected	0 - Exploitation Detected	Not Applicable

目前微软已经对此漏洞发布了专门的例行外补丁和通告，相关的技术细节已通知安全合作伙伴，奇安信威胁情报中心确认漏洞的存在，强烈建议用户更新软件补丁以抵御此威胁的影响。

从不同处的情报维度表明，无论是该漏洞的发现者默认转推的一条对该漏洞的归因到 Darkhotel APT 组织的推文；

还是卡巴斯基高级威胁研究团队 GReAT 负责人的推文，都表明该在野 0day 漏洞被 DarkHotel 组织利用来攻击的可能性极高。

因此奇安信威胁情报中心在得知此次事件后，进行研判得到结果表明，在实施针对性目标攻击打击的各国网军中，DarkHotel 为其中一个尤爱使用 0day 漏洞进行攻击的 APT 组织，从此前的 vbscript 0day CVE-2018-8174，CVE-2018-8373 等，可明确该组织会针对目标，购买或制作定制化的网络漏洞武器，此漏洞暴露需要引起重视，尤其是重点单位。

DarkHotel，维基百科指称是一个来自韩国的 APT 组织，其起初攻击目标是入住高端酒店的商务人士或有关国家政要，攻击入口是酒店 WiFi 网络。而如今，Darkhotel 已经使用各种方式对目标进行持续性攻击至今，目标涉及中国、俄罗斯、朝鲜、日本等，是一个具备高强战力的 APT 组织。

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 ID**	CVE-2019-1367
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

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。

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或者网站，成功触发漏洞后便可获得与当前用户相同的用户权限，攻击者可以安装恶意程序，增加、删除、更改或查看数据。

影响面评估

根据百度浏览器市场份额数据显示，IE 11 目前市场占比大约为 7.26%，该数据量级结合中国网民基数实际上很是惊人。

对于国内而言，在大部分的政企单位内网，很多人员依然使用着 IE，仅仅因为办公系统兼容性不够，并且还使用 jscript 作为脚本引擎的网站。

处置建议

更新系统补丁：
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

缓解措施

限制对 JScript.dll 的访问

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
```

时间线

2019-09-23 微软发布安全公告并紧急推出修复补丁
2019-09-24 奇安信威胁情报中心评估影响面并发布风险提示
2019-09-25 奇安信威胁情报中心根据外部情报补充风险提示

参考资料

https://support.microsoft.com/en-us/help/4522007/cumulative-security-update-for-internet-explorer
https://en.wikipedia.org/wiki/DarkHotel