【漏洞总结】2019微软5月漏洞总结

原创：小白 青藤实验室

0x00 概述

微软已发布5月针对其多个产品中已发现并解决的漏洞的安全更新，本次更新共涉及漏洞79个，其22个漏洞评级为 Critical，57个漏洞评级为 Important。影响 Windows、.NET Framewor Office、ASP.NET Core 等。

此次更新中存在一个 RDP 远程代码执行漏洞，未经认证的恶意攻击者通过向目标主机RDP服务所端口发送精心构造的请求，即可在目标主机执行任意代码。此漏洞是身份验证，无需用户交互，利用门槛低，危害大且攻击者可通过该漏洞横向蠕虫传播，感染大量主机，危害效果可堪比2017年WannaCry等具备勒索能力的恶意程序.目前官方暂未公开漏洞细节，建议受影响用户尽快安装补丁进行更新，修复此漏洞。

0x01 漏洞详情

以下漏洞级别为 Critical

1. Windows DHCP 服务器远程代码执行漏洞

当处理经特殊设计的数据包时，Windows Server DHCP 服务中存在内存损坏漏洞。成功利用此洞的攻击者可以在 DHCP 服务器上运行任意代码。

- CVE-2019-0725 - Windows DHCP Server Remote Code Execution Vulnerability

2. 脚本引擎内存损坏漏洞

脚本引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用权限。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者便可控制受影响的系统。攻者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

- CVE-2019-0884 - Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0911 - Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0912 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0913 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0914 - Chakra Scripting Engine Memory Corruption Vulnerability

- CVE-2019-0915 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0916 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0917 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0918 - Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0922 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0924 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0925 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-0927 - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-093[illegible] - Chakra Scripting Engine Memory Corruption Vulnerability
- CVE-2019-093[illegible] - Chakra Scripting Engine Memory Corruption Vulnerability

3. GDI+ 远程代码执行漏洞

Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有全用户权限的新帐户。与拥有管理用户权限的用户相比，被配置为拥有较少权限的用户受到的影响小。

- CVE-2019-0903 -GDI+ Remote Code Execution Vulnerability

4. Microsoft 浏览器内存损坏漏洞

Microsoft 浏览器不正确访问内存中的对象时，存在远程代执行漏洞。该漏洞可能以一种使攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当用户相同的用户权限。如果当前用户使用管理用户权限登录，那么攻击者便可控制受影响的系统。击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

- CVE-2019-092[illegible] - Microsoft Edge Memory Corruption Vulnerability
- CVE-2019-0929 - Internet Explorer Memory Corruption Vulnerability
- CVE-2019-0940 - Microsoft Browser Memory Corruption Vulnerability

5. Microsoft Word 远程代码执行漏洞

Microsoft Word 软件无法正确处理内存中的对象时，其中存在远程代执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的文件在当前用户的安全上下文中执行操作。例如，文件可以代表登用户使用与当前用户相同的权限执行操作。

- CVE-2019-0953 - Microsoft Word Remote Code Execution Vulnerability

以下漏洞级别为Important

6. Windows NDIS 权限提升漏洞

当 ndis.sys 将内存复制到缓冲区之前无法检查缓冲区长度时，网络驱动程序接口规范（NDIS）中
在特权提升漏洞。
若要利用此漏洞，在本地攻击情形下，攻击者可以运行经特殊设计的应用程序以提升攻击者的特权
别。成功利用此漏洞的攻击者可以在提升的上下文中运行进程。

- CVE-2019-0707 - Windows NDIS Elevation of Privilege Vulnerability

7. Diagnostic Hub Standard Collector, Visual Studio Standard Collect 权限提升漏洞

Diagnostic Hub Standard Collector, Visual Studio Standard Collector 允许在任意位置
文件时，存在权限提升漏洞。

- CVE-2019-0727 - Diagnostic Hub Standard Collector, Visual Studio Standard Colle Elevation of Privilege Vulnerability

8. Windows Defender Application Control 安全功能绕过漏洞

Windows Defender Application Control (WDA中存在可能允许攻击者绕过 WDAC 强制执行的安
全功能绕过漏洞。成功利用此漏洞的攻击者可以避开计算机上 Windows PowerShell约束语言模
式。

- CVE-2019-0733 - Windows Defender Application Control Security Feature Byp Vulnerability

9. Windows 权限提升漏洞

当中间人攻击者能够使用 Kerberos 成功地解码和替换身份验证请求，从而允许将攻击者验证为管
员时，Microsoft Windows 中存在特权提升漏洞。

- CVE-2019-0734 - Windows Elevation of Privilege Vulnerability

10. Windows GDI 信息泄漏漏洞

Windows GDI 组件不正确披露其内存中的内容时，存在信息泄漏漏洞。成功利用此漏洞的攻击者
以获取信息，从而进一步入侵用户系统。

- CVE-2019-0758 - Windows GDI Information Disclosure Vulnerability
- CVE-2019-0882 - Windows GDI Information Disclosure Vulnerability
- CVE-2019-0961 - Windows GDI Information Disclosure Vulnerability

11. Microsoft SQL Server Analysis Services 信息泄露漏洞

Microsoft SQL Server Analysis Services 不正确地执行元数据权限时，其中存在信息泄漏漏洞
成功利用此漏洞的攻击者可以查询他们没有访问权限的表或列。

- CVE-2019-0819 - Microsoft SQL Server Analysis Services Information Disclos

Vulnerability

12. .NET Framework 和 .NET Core 拒绝服务漏洞

当 .NET Framework 和 .NET Core 不正确处理 RegEx 字符串时当 .NET Framework 不正确地处理堆内存中的对象时 ,存在拒绝服务漏洞。成功利用此漏洞的攻击者可能会导致 .NET 应用程序拒绝服务。此漏洞可以被远程利用，而无需进行身份验证。

- CVE-2019-0820 -.NET Framework and .NET Core Denial of Service Vulnerability
- CVE-2019-0864 -.NET Framework Denial of Service Vulnerability
- CVE-2019-0980 -.NET Framework and .NET Core Denial of Service Vulnerability
- CVE-2019-0981 -.NET Framework and .NET Core Denial of Service Vulnerability

13. Windows Error Reporting 权限提升漏洞

Windows Error Reportin (WER) 处理文件的方式中存在权限提升漏洞。成功利用此漏洞的攻击可以在内核模式中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有理员特权的新帐户。

- CVE-2019-0863 - Windows Error Reporting Elevation of Privilege Vulnerability

14. Azure DevOps Server and Team Foundation Serv跨站脚本漏洞

Azure DevOps Server 和 Team Foundation Server 未正确清理用户提供的输入时，存在跨站脚本（XSS）漏洞。 经过身份验证的攻击者可以通过向 Azure DevOps Server 或 Team Foundation Server发送特制的有效负载来利用此漏洞，每当用户访问受感染的页面时有效负载就会在用户上下文中执行。

- CVE-2019-0872 - Azure DevOps Server and Team Foundation Server Cross-Scripting Vulnerability
- CVE-2019-0979 - Azure DevOps Server and Team Foundation Server Cross-Scripting Vulnerability

15. Windows 内核权限提升漏洞

Windows 内核不正确地处理密钥枚举时，存在特权提升漏洞。成功利用该漏洞的攻击者可以在目系统上获得特权提升。

- CVE-2019-0881 - Windows Kernel Elevation of Privilege Vulnerability

16. Windows OLE 远程代码执行漏洞

当 Microsoft Windows OLE 无法正确验证用户输入时，存在远程执行代码漏洞。攻击者可以利此漏洞以执行恶意代码。

- CVE-2019-0885 - Windows OLE Remote Code Execution Vulnerability

17. Windows Hyper-V 信息泄漏漏洞

当主机操作系统上的 Windows Hyper-V 无法正确验证来宾操作系统上已通过身份验证的用户的入时，存在信息泄漏漏洞。为了利用此漏洞，来宾操作系统上的攻击者可以运行经过特殊设计的可Hyper-V 主机操作系统泄漏内存信息的应用程序。

- CVE-2019-0886 - Windows Hyper-V Information Disclosure Vulnerability

18. Jet 数据库引擎远程代码执行漏洞

Windows Jet 数据库引擎不正确地处理内存中的对象时，存在远程执行代码漏洞。成功利用此漏的攻击者可以在受害者系统上执行任意代码。

- CVE-2019-0889 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0890 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0891 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0893 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0894 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0895 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0896 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0897 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0898 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0899 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0900 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0901 - Jet Database Engine Remote Code Execution Vulnerability
- CVE-2019-0902 - Jet Database Engine Remote Code Execution Vulnerability

19. Win32k 权限提升漏洞

Win32k 组件无法正确处理内存中的对象时，Windows 中存在权限提升漏洞。成功利用此漏洞的击者可以在内核模式中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建有完全用户权限的新帐户。

- CVE-2019-0892 - Win32k Elevation of Privilege Vulnerability

20. Internet Explorer 欺骗漏洞

当 Internet Explorer 不正确地处理 URL 时，存在欺骗漏洞。成功利用此漏洞的攻击者可以通过用户重定向到经特殊设计的网站来诱骗用户。经特殊设计的网站可以包含欺骗内容，也可以用作关攻击与 Web 服务中其他漏洞的枢纽。

- CVE-2019-0921 - Internet Explorer Spoofing Vulnerability

21. 脚本引擎内存损坏漏洞

脚本引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用
的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用
权限。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者便可控制受影响的系统。攻
者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

- CVE-2019-0923 - Chakra Scripting Engine Memory Corruption Vulnerability

22. Internet Explorer 信息泄漏漏洞

Internet Explorer 不正确地处理内存中的对象时，存在信息泄漏漏洞。成功利用此漏洞的攻击者
以获取信息，从而进一步入侵用户系统。

- CVE-2019-0930 - Internet Explorer Information Disclosure Vulnerability

23. Windows Storage Service 权限提升漏洞

Windows Storage Servic不当处理文件操作时，存在特权提升漏洞。成功利用这个漏洞的攻击者
以在受害者系统上获得特权提升。

- CVE-2019-0931 - Windows Storage Service Elevation of Privilege Vulnerability

24. Skype for Android 信息泄漏漏洞

Skype for Android 中存在信息泄漏漏洞。利用此漏洞的攻击者可以在用户不知情的情况下窃
Android 版 Skype 用户的对话。

若要利用此漏洞，攻击者需要向安装了 Android 版 Skype 且与蓝牙设备配对的 Android 手机拨
电话。

- CVE-2019-0932 - Skype for Android Information Disclosure Vulnerability

25. Windows 权限提升漏洞

Windows 未能正确处理某些符号链接时，Microsoft Windows 中存在特权提升漏洞。成功利用
漏洞的攻击者可能会将某些项目设置为在更高级别上运行，进而提升权限。

- CVE-2019-0936 - Windows Elevation of Privilege Vulnerability

26. Microsoft Edge 权限提升漏洞

Microsoft Edge 中存在特权提升漏洞，攻击者可以利用此漏洞跳出浏览器中的 AppContainer
盒。成功利用此漏洞的攻击者可以获得特权提升并跳出 Edge AppContainer 沙盒。

- CVE-2019-0938 -WindowsEdge Elevation of Privilege Vulnerability

27. Unified Write Filter 权限提升漏洞

Unified Write Filter (UWF) 功能不正确地限制对注册表的访问时，其中存在特权提升漏洞。成功

用此漏洞的攻击者可以在没有管理员权限的情况下更改受 UWF 保护的注册表项。

- CVE-2019-0942 - Unified Write Filter Elevation of Privilege Vulnerability

28. Microsoft Office Access Connectivity Engine 远程代码执行漏洞

Microsoft Office Access Connectivity Engine 不当处理内存中的对象时，存在远程代码执行
洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。

- CVE-2019-0945 -Microsoft Office Access Connectivity Engine Remote Code Execut Vulnerability
- CVE-2019-0946 -Microsoft Office Access Connectivity Engine Remote Code Execut Vulnerability
- CVE-2019-0947 -Microsoft Office Access Connectivity Engine Remote Code Execut Vulnerability

29. Microsoft SharePoint 欺骗漏洞

Microsoft SharePoint Server 未正确清理发往受影响的 SharePoint 服务器的经特殊设计的 W
请求时，存在欺骗漏洞。经过身份验证的攻击者可能通过向受影响的 SharePoint 服务器发送经
殊设计的请求来利用此漏洞。

- CVE-2019-0949 - Microsoft SharePoint Spoofing Vulnerability
- CVE-2019-0950 -Microsoft SharePoint Spoofing Vulnerability
- CVE-2019-0951 -Microsoft SharePoint Spoofing Vulnerability

30. Microsoft SharePoint Server 远程代执行漏洞

Microsoft SharePoint Server 无法正确识别和筛选不安全的 ASP.NET Web 控件时，存在远程
码执行漏洞。成功利用此漏洞的经过身份验证的攻击者可以使用经特殊设计的页面在 SharePo
应用程序池进程的安全上下文中执行操作。

- CVE-2019-0952 - Microsoft SharePoint Server Remote Code Execution Vulnerability

31. Microsoft SharePoint Serve 信息泄露漏洞

Microsoft SharePoint Server 未正确清理发往受影响的 SharePoint 服务器的经特殊设计的 W
请求时，存在信息泄漏漏洞。经过身份验证的攻击者可能通过向受影响的 SharePoint 服务器发
经特殊设计的请求来利用此漏洞。
成功利用这些漏洞的攻击者可能在受影响的系统上执行跨站脚本攻击，并在当前用户的安全上下文
运行脚本。

- CVE-2019-0956 - Microsoft SharePoint Server Information Disclosure Vulnerability

32. Microsoft SharePoint Serve 权限提升漏洞

Microsoft SharePoint Server 未正确审查发往受影响的 SharePoint 服务器的经特殊设计的 W
请求时，存在特权提升漏洞。经过身份验证的攻击者可能通过向受影响的 SharePoint 服务器发
经特殊设计的请求来利用此漏洞。
成功利用这些漏洞的攻击者可能在受影响的系统上执行跨站脚本攻击，并在当前用户的安全上下文
运行脚本。

- CVE-2019-0957 - Microsoft SharePoiElevation of Privilege Vulnerability
- CVE-2019-0958 -Microsoft SharePoinElevation of Privilege Vulnerability

33. Microsoft Office SharePoint XSS 漏洞

Microsoft SharePoint Server 未正确审查发往受影响的 SharePoint 服务器的经特殊设计的 W
请求时，存在跨站点脚本 (XSS) 漏洞。经过身份验证的攻击者可能通过向受影响的 SharePoint
务器发送经特殊设计的请求来利用此漏洞。成功利用这些漏洞的攻击者可能在受影响的系统上执行跨
站脚本攻击，并在当前用户的安全上下文中运行脚本。

- CVE-2019-0963 - Microsoft Office SharePoint XSS Vulnerability

34. Azure DevOps Server and Team Foundation Server 信息泄漏洞

Azure DevOps Server 和 Microsoft Team Foundation Server 未正确清理发往受影响的服
的经特殊设计的身份验证请求时，存在信息泄漏漏洞。成功利用此漏洞的攻击者可以在易受攻击的
务器上执行恶意代码。

- CVE-2019-0971 - Azure DevOps Server and Team Foundation Server Informa
  Disclosure Vulnerability

35. ASP.NET Core 拒绝服务漏洞

当 ASP.NET Core 不正确处理 Web 请求时，存在拒绝服务漏洞。成功利用此漏洞的攻击者可能
导致 ASP.NET Core Web 应用程序拒绝服务。此漏洞可以被远程利用，而无需进行身份验证。

- CVE-2019-0982 - AS.NET Core Denial of Service Vulnerability

36. Internet Explorer 安全功能绕过漏洞

当 urlmon.dll 不正确地处理某些 Web 查询标记时，存在安全功能绕过漏洞。此漏洞允许 Interr
Explorer 绕过以特定方式下载或创建的文件的 Web 警告或限制标记。

- CVE-2019-0995 - Internet Explorer Security Feature Bypass Vulnerability

37. Microsoft Azure AD Connect 权限提升漏洞

Microsoft Azure Active Directory Connect 内部版本 1.3.20.0 中存在特权提升漏洞，该漏洞
许攻击者在特权帐户上下文中执行两个 PowerShell Cmdlet，并执行特权操作。

- CVE-2019-1000 - Microsoft Azure AD Connect Elevation of Privilege Vulnerability