**附件**

**一、 漏洞介绍**

       本次漏洞公告涉及Microsoft Windows系统 、ActiveX插件、Internet Explorer浏览器、Chakra 脚本引擎、Microsoft XML Core Services分析器、TFTP 服务器、VBScript 引擎、Windows DHCP 客户端等Windows平台下应用软件和组件。漏洞详情如下：

       1、Windows ActiveX 远程代码执行漏洞（CNNVD-201903-377、CVE-2019-0784）

       漏洞简介：ActiveX处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可导致攻击者在对象内存中执行任意代码。成功利用该漏洞的攻击者可以获得与当前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，成功利用此漏洞的攻击者便可控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

       2、Internet Explorer 内存损坏漏洞（CNNVD-201903-435、CVE-2019-0763）

       漏洞简介：当 Internet Explorer 不正确地访问内存中的对象时会触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限，从而进一步安装程序、查看、更改或删除数据、创建新帐户。

       3、Chakra 脚本引擎内存损坏漏洞（CNNVD-201903-421、CVE-2019-0592）

       漏洞简介：Chakra 脚本引擎在 Microsoft Edge 中处理内存中的对象的时可能触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理权限登录，攻击者便可以任意安装程序、查看、更改或删除数据。

       4、MS XML 远程代码执行漏洞（CNNVD-201903-385、CVE-2019-0756）

       漏洞简介：当 Microsoft XML Core Services分析器处理用户输入时，存在远程代码执行漏洞。攻击者需要诱使用户点击电子邮件或即时消息中的链接以使用户链接到存在恶意代码的网站。当 Internet Explorer 分析 XML 内容时，攻击者可以远程运行恶意代码控制用户的系统。

       5、Windows 部署服务 TFTP 服务器远程代码执行漏洞（CNNVD-201903-384、CVE-2019-0603）

       漏洞简介：Windows 部署服务 TFTP 服务器在处理内存中的对象时存在远程代码执行漏洞。攻击者可以创建经特殊设计的请求，提升 Windows 权限，从而执行恶意代码。

       6、Windows VBScript 引擎远程代码执行漏洞（CNNVD-201903-386、CVE-2019-0666）、（CNNVD-201903-398、CVE-2019-0667）

漏洞简介：VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。成功利用该漏洞的攻击者可以获得与当前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，如果当前用户使用管理权限登录，攻击者便可以任意安装程序、查看、更改或删除数据。

       7、Windows DHCP 客户端远程代码执行漏洞（CNNVD-201903-375、CVE-2019-0697）、（CNNVD-201903-389、CVE-2019-0698）、（CNNVD-201903-391、CVE-2019-0726）

       漏洞简介：当攻击者向Windows DHCP服务器发送经特殊设计的 DHCP 数据包时，会触发该漏洞。成功利用此漏洞的攻击者可以在服务器上执行任意代码。

       8、Win32k 信息泄漏漏洞（CNNVD-201903-373、CVE-2019-0776）、（CNNVD-201903-452、CVE-2019-0808）

       漏洞简介：当 Win32k 组件不正确地提供内核信息时，存在信息泄漏漏洞。成功利用此漏洞的攻击者可以获取用户信息，从而进一步入侵用户系统。要利用此漏洞，攻击者需登录系统，运行专门设计的应用程序，该应用程序可以利用漏洞控制受影响的系统。

       9、Microsoft Edge 内存损坏漏洞（CNNVD-201903-448、CVE-2019-0779）

       漏洞简介：当 Microsoft Edge 不正确地访问内存中的对象时会触发该漏洞。成功利用该漏洞的攻击者可以获得与当前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，攻击者便可以控制受影响的系统。攻击者可任意安装程序、查看、更改或删除数据、或者创建新帐户。

**二、修复建议**

       目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，采取修补措施。微软官方链接地址如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 漏洞名称 | 官方链接 |
| 1 | Windows ActiveX 远程代码执行漏洞（CNNVD-201903-377、CVE-2019-0784） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0784 |
| 2 | Internet Explorer 内存损坏漏洞（CNNVD-201903-435、CVE-2019-0763） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0763 |
| 3 | Chakra 脚本引擎内存损坏漏洞（CNNVD-201903-421、CVE-2019-0592） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0592 |
| 4 | MS XML 远程代码执行漏洞（CNNVD-201903-385、CVE-2019-0756） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0756 |
| 5 | Windows 部署服务 TFTP 服务器远程代码执行漏洞（CNNVD-201903-384、CVE-2019-0603） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0603 |
| 6 | Windows VBScript 引擎远程代码执行漏洞（CNNVD-201903-386、CVE-2019-0666）、（CNNVD-201903-398、CVE-2019-0667） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0666  https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0667 |
| 7 | Windows DHCP 客户端远程代码执行漏洞（CNNVD-201903-375、CVE-2019-0697）、（CNNVD-201903-389、CVE-2019-0698）、（CNNVD-201903-391、CVE-2019-0726） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0697  https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0698  https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0726 |
| 8 | Win32k 信息泄漏漏洞（CNNVD-201903-373、CVE-2019-0776）、（CNNVD-201903-452、CVE-2019-0808） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0776  https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0808 |
| 9 | Microsoft Edge 内存损坏漏洞（CNNVD-201903-448、CVE-2019-0779） | https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0779 |