微软2017年10月安全公告

**安全公告编号:CNTA-2017-0072**

10月10日，微软发布了2017年10月份的月度例行安全公告，修复了其多款产品存在的220个安全漏洞。受影响的产品包括Windows 10 v1703（27个）、Windows 10 v1607 and Windows Server 2016（27个）、Windows 10 v1511（26个）、Windows 10 RTM（27个）、Windows 8.1 and Windows Server 2012 R2（23个）、Windows Server 2012（20个）、Windows 7 and Windows Server 2008 R2（20个）、Windows Server 2008（20个）、Internet Explorer (5个)、Microsoft Edg（17个）和Office（8个）。

利用上述漏洞，攻击者可以执行远程代码，提升权限，获得敏感信息或进行拒绝服务攻击等。CNVD提醒广大Microsoft用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

|  |  |  |  |
| --- | --- | --- | --- |
| **CVE编号** | **公告标题和摘要** | **最高严重等级**  **和漏洞影响** | **受影响的软件** |
| CVE-2017-11780 | **Microsoft Windows SMB Server远程代码执行漏洞**  远程攻击者可通过向目标SMBv1服务器发送特制的数  据包利用该漏洞在目标服务器上执行代码。 | 严重  远程执行代码 | Microsoft Windows |
| CVE-2017-11771 | **Microsoft Windows Search远程代码执行漏洞**  远程攻击者可通过向Windows Search服务发送特制  的消息利用该漏洞在目标系统上执行任意代码或造成拒绝服务。 | 严重  远程执行代码 | Microsoft Windows |
| CVE-2017-11779 | **Windows Domain Name System (DNS) DNSAPI.dll**  **文件远程代码执行漏洞**  DNSAPI.dll无法正确处理DNS响应。攻击者将使用恶  意DNS服务器将恶意的DNS响应发送到目标。 | 严重  远程执行代码 | Microsoft Windows |
| CVE-2017-11762 | **Graphics Comp远程代码执行漏洞**  经过身份验证的攻击者可以通过发送特制请求利用该漏  洞在受影响的SharePoint服务器上代表用户采取行动，  如更改权限和删除内容，并在用户浏览器中注入恶意的内容。 | 严重  远程执行代码 | Microsoft Windows |
| CVE-2017-11796 | **浏览器脚本引擎远程代码执行漏洞**  攻击者可以托管一个特制的网站，通过受影响的Microsoft浏  览器，然后说服用户查看网站。攻击者还可以利用受损网站  或通过添加可能利用此漏洞的特制内容来接受或托管用户提  供的内容或广告的网站。攻击者还可以嵌入一个标记为“安全  的”的ActiveX控件应用程序或Office文档中承载IE或Edge渲染  引擎的初始化。 | 严重  远程执行代码 | Microsoft Edge  Chakra Core |
| CVE-2017-11826 | **Office远程代码执行漏洞**  利用这些漏洞需要用户打开受影响的Microsoft Office软件版本  的特制文件。  网络场景 - 攻击者使用该漏洞托管恶意网站，然后说服用户访问  该网站或攻击者利用其他提供商托管广告的受损网站和/或网站。  电子邮件场景 - 攻击者发送特制文件并说服用户打开文件。 | 重要  远程执行代码 | Microsoft Office |
| CVE-2017-11777 | **SharePoint权限提升漏洞**  经过身份验证的攻击者可以通过发送特制请求来利用此漏洞到受  影响的SharePoint服务器。这些攻击可能允许攻击者读取内容或  无权阅读，使用受害者的身份在SharePoint网站上采取行动代表  用户，如更改权限和删除内容，并注入恶意用户浏览器中的内容。 | 重要  权限提升 | Microsoft SharePoint |

**参考信息：**

<https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/313ae481-3088-e711-80e2-000d3a32fc99>