2017 年 10 月 10 日，星期二

Microsoft 星期二补丁 - 2017 年 10 月

Microsoft 已经针对各种产品中发现和解决的漏洞发布了月度安全公告集。本月发布的安全公告可修复 63 个新漏洞，其中 28 个为严重等级漏洞，35 个为重要等级漏洞。受这些漏洞影响的有图形、Edge、Internet Explorer、Office、Sharepoint、Windows 图形显示界面、Windows 内核模式驱动程序等等。

评为严重等级的漏洞

以下是 Microsoft 评为“严重”等级的漏洞：

- CVE-2017-11813 - Internet Explorer 内存损坏漏洞
- CVE-2017-11822 - Internet Explorer 内存损坏漏洞
- CVE-2017-11762 - Microsoft 图形远程代码执行漏洞
- CVE-2017-11763 - Microsoft 图形远程代码执行漏洞
- CVE-2017-11797 - 脚本引擎信息泄露漏洞
- CVE-2017-11767 - 脚本引擎内存损坏漏洞
- CVE-2017-11792 - 脚本引擎内存损坏漏洞
- CVE-2017-11793 - 脚本引擎内存损坏漏洞
- CVE-2017-11796 - 脚本引擎内存损坏漏洞
- CVE-2017-11798 - 脚本引擎内存损坏漏洞
- CVE-2017-11799 - 脚本引擎内存损坏漏洞
- CVE-2017-11800 - 脚本引擎内存损坏漏洞
- CVE-2017-11801 - 脚本引擎内存损坏漏洞
- CVE-2017-11802 - 脚本引擎内存损坏漏洞
- CVE-2017-11804 - 脚本引擎内存损坏漏洞
- CVE-2017-11805 - 脚本引擎内存损坏漏洞
- CVE-2017-11806 - 脚本引擎内存损坏漏洞
- CVE-2017-11807 - 脚本引擎内存损坏漏洞
- CVE-2017-11808 - 脚本引擎内存损坏漏洞
- CVE-2017-11809 - 脚本引擎内存损坏漏洞
- CVE-2017-11810 - 脚本引擎内存损坏漏洞
- CVE-2017-11811 - 脚本引擎内存损坏漏洞
- CVE-2017-11812 - 脚本引擎内存损坏漏洞

- CVE-2017-11821 - 脚本引擎内存损坏漏洞
- CVE-2017-11779 - Windows DNSAPI 远程代码执行漏洞
- CVE-2017-11771 - Windows Search 远程代码执行漏洞
- CVE-2017-8727 - Windows Shell 内存损坏漏洞
- CVE-2017-11819 - Windows Shell 远程代码执行漏洞

CVE-2017-11813、CVE-2017-11822 - Internet Explorer 内存损坏漏洞

在 Internet Explorer 中发现了两个漏洞，它们可能会在当前用户环境下引发远程代码执行。造成这些漏洞的原因，是由于程序在尝试呈现网页时对内存中的对象处理不当。例如，如果用户访问利用其中一个漏洞特殊设计的网页，则这两个漏洞均会被利用。

CVE-2017-11762、CVE-2017-11763 - Microsoft 图形远程代码执行漏洞

在 Microsoft 图形组件的字体库中发现了两个漏洞，攻击者可能会利用这些漏洞执行任意代码。出现这些漏洞是因为字体库对网页或文档内专门嵌入的字体处理不当。如果用户导航至恶意网页或者打开利用这些漏洞的经特殊设计的文档，则这两个漏洞会被利用。

多个 CVE - 脚本引擎内存损坏漏洞

在 Edge 和 Internet Explorer 的脚本引擎中发现了多个漏洞，攻击者可能会利用这些漏洞远程执行任意代码。出现这些漏洞是因为 Edge 和 Internet Explorer 中的脚本引擎对内存中的对象处理不当。因此，如果成功利用这些漏洞，会导致在当前用户所处的环境下执行任意代码。这些漏洞可能会被利用的情况包括基于 Web 的攻击，在此类攻击中，用户导航至旨在利用这些漏洞的恶意网页，或者在某些情况下打开包含标记为“可安全初始化”的嵌入式 ActiveX 控件的 Microsoft Office 文档。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11767
- CVE-2017-11792
- CVE-2017-11793
- CVE-2017-11796
- CVE-2017-11797
- CVE-2017-11798

- CVE-2017-11799
- CVE-2017-11800
- CVE-2017-11801
- CVE-2017-11802
- CVE-2017-11804
- CVE-2017-11805
- CVE-2017-11806
- CVE-2017-11807
- CVE-2017-11808
- CVE-2017-11809
- CVE-2017-11810
- CVE-2017-11811
- CVE-2017-11812
- CVE-2017-11821

CVE-2017-11779 - Windows DNSAPI 远程代码执行漏洞

在 Windows DNS 中发现了一个远程代码执行漏洞，攻击者可能会利用此漏洞在本地系统帐户环境下执行任意代码。DNSAPI.dll 中出现此漏洞是因为对 DNS 响应处理不当。此漏洞可能会被利用的一种情况是：攻击者利用恶意 DNS 服务器将经特殊设计的 DNS 响应传输到目标。

CVE-2017-11771 - Windows Search 远程代码执行漏洞

在 Window Search 中发现了一个任意代码执行漏洞，攻击者可能会利用此漏洞提升其权限，继而在权限提升后的环境下执行代码。出现此漏洞是因为对内存中的对象处理不当。要利用此漏洞，攻击者需要具备对目标主机的访问权限，或者通过 SMB 连接远程触发此漏洞。

CVE-2017-8727 - Windows Shell 内存损坏漏洞

在 Internet Explorer 中发现了一个远程代码执行漏洞，攻击者可能会利用此漏洞在当前用户环境下执行任意代码。出现此漏洞是因为 Internet Explorer 未通过 Microsoft Windows 文本服务框架正确访问内存中的对象。攻击者可能会创建一个经特殊设计的网页来利用此漏洞，然后利用社会工程方式让用户访问该网页来达到攻击用户的目的。此外，攻击者可能会利用用于展示用户提供的内容或广告的易受攻击或已受攻击的网站或站点来利用此漏洞，攻击用户。

CVE-2017-11819 - Windows Shell 远程代码执行漏洞

在 Microsoft 网络浏览器中发现了一个远程代码执行漏洞，出现此漏洞是因为对内存中的对象处理不当。成功利用此漏洞的攻击者可在当前用户环境下执行任意代码。攻击者可能会通过设计特殊网页并运用社会工程方式让用户访问此网页，来利用此漏洞攻击用户。其他情况包括攻击者利用用于展示用户提供的内容或广告的易受攻击或已受攻击的网站或站点来利用此漏洞，攻击用户。

评为重要等级的漏洞

以下是 Microsoft 评为“重要”等级的漏洞：

- CVE-2017-11790 - Internet Explorer 信息泄露漏洞
- CVE-2017-11794 - Microsoft Edge 信息泄露漏洞
- CVE-2017-8726 - Microsoft Edge 内存损坏漏洞
- CVE-2017-8693 - Microsoft 图形信息泄露漏洞
- CVE-2017-8717 - Microsoft JET 数据库引擎远程代码执行漏洞
- CVE-2017-8718 - Microsoft JET 数据库引擎远程代码执行漏洞
- CVE-2017-11826 - Microsoft Office 内存损坏漏洞
- CVE-2017-11825 - Microsoft Office 远程代码执行漏洞
- CVE-2017-11775 - Microsoft Office SharePoint XSS 漏洞
- CVE-2017-11777 - Microsoft Office SharePoint XSS 漏洞
- CVE-2017-11820 - Microsoft Office SharePoint XSS 漏洞
- CVE-2017-11776 - Microsoft Outlook 信息泄露漏洞
- CVE-2017-11774 - Microsoft Outlook 安全功能绕过漏洞
- CVE-2017-11772 - Microsoft Search 信息泄露漏洞
- CVE-2017-11823 - Microsoft Windows 安全功能绕过漏洞
- CVE-2017-11786 - Skype for Business 权限提升漏洞
- CVE-2017-11769 - TRIE 远程代码执行漏洞
- CVE-2017-8689 - Win32k 权限提升漏洞
- CVE-2017-8694 - Win32k 权限提升漏洞
- CVE-2017-11783 - Windows 权限提升漏洞
- CVE-2017-11816 - Windows GDI 信息泄露漏洞

- CVE-2017-11824 - Windows 图形组件权限提升漏洞
- CVE-2017-11817 - Windows 信息泄露漏洞
- CVE-2017-11765 - Windows 内核信息泄露漏洞
- CVE-2017-11784 - Windows 内核信息泄露漏洞
- CVE-2017-11785 - Windows 内核信息泄露漏洞
- CVE-2017-11814 - Windows 内核信息泄露漏洞
- CVE-2017-8715 - Windows 安全功能绕过漏洞
- CVE-2017-11781 - Windows SMB 拒绝服务漏洞
- CVE-2017-11782 - Windows SMB 权限提升漏洞
- CVE-2017-11815 - Windows SMB 信息泄露漏洞
- CVE-2017-11780 - Windows SMB 远程代码执行漏洞
- CVE-2017-11818 - Windows Storage 安全功能绕过漏洞
- CVE-2017-8703 - 适用于 Linux 的 Windows 子系统拒绝服务漏洞
- CVE-2017-11829 - Windows 更新传递优化权限提升漏洞

CVE-2017-11790 - Internet Explorer 信息泄露漏洞

在 Internet Explorer 中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞获取可用于进一步攻击受影响系统的信息。出现此漏洞是因为 Internet Explorer 对内存中的对象处理不当。如果用户导航至受攻击者控制的网页，则可能会被攻击者利用发起攻击。此外，如果用户导航至托管用户生成内容的站点，也可能会被攻击者利用发起攻击。

CVE-2017-11794 - Microsoft Edge 信息披露漏洞

在 Edge 中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞获取可用于进一步攻击受影响系统的信息。出现此漏洞是因为 Edge 对内存中的对象处理不当。如果用户导航至受攻击者控制的网页，则可能会被攻击者利用发起攻击。此外，如果用户导航至托管用户生成内容的站点，也可能会被攻击者利用发起攻击。

CVE-2017-8726 - Microsoft Edge 内存损坏漏洞

在 Edge 中发现了一个远程代码执行漏洞，攻击者可能会利用此漏洞在当前用户环境下执行任意代码。出现此漏洞是因为 Edge 对内存中的对象处理不当。攻击者可能会利用此漏洞攻

击用户的情况包括：当用户导航至受攻击者控制的经特殊设计的网页时，可能会受到基于 Web 的攻击。其他可能的情况包括用户打开包含标记为“可安全初始化”的嵌入式 ActiveX 控件的 Microsoft Office 文档。

CVE-2017-8693 - Microsoft 图形信息泄露漏洞

在 Microsoft Windows 图形组件中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞获取可用于进一步攻击受影响系统的信息。出现此漏洞是因为图形组件对内存中的对象处理不当。如果某个经过身份验证的用户要启动旨在利用此漏洞的经特殊设计的可执行文件，则此漏洞可能会被利用。

CVE-2017-8717、CVE-2017-8718 - Microsoft JET 数据库引擎远程代码执行漏洞

在 Microsoft JET 数据库引擎中发现了两个任意代码执行漏洞，攻击者可能会利用这些漏洞在当前用户环境下执行任意代码。出现这些漏洞是因为触发了缓冲区溢出条件。攻击者若想成功利用这些漏洞，需要用户在受影响的 Windows 版本上打开或预览经特殊设计的 Microsoft Excel 文档。基于邮件的攻击是用户最有可能受到攻击的情况，在此类攻击中，攻击者会向受害者发送经特殊设计的 Excel 文档。

CVE-2017-11826 - Microsoft Office 内存损坏漏洞

在 Microsoft Office 中发现了一个漏洞，攻击者可能会利用此漏洞在受影响系统上执行任意代码。出现这个漏洞是因为 Office 对内存中的对象处理不当。如果用户打开经特殊设计的恶意 Office 文件，可能会导致此漏洞被利用，使攻击者可以在当前用户环境中执行攻击者选择的任意代码。这类攻击情况包括基于邮件的攻击（攻击者向受害者发送包含恶意附件的邮件）或基于 Web 的攻击（用户下载并打开恶意 Office 文件）。请注意，在某些条件下，预览窗格也是一种攻击媒介。

CVE-2017-11825 - Microsoft Office 远程代码执行漏洞

在 Microsoft Office 中发现了一个漏洞，攻击者可能会利用此漏洞在受影响系统上执行任意代码。出现这个漏洞是因为 Office 对内存中的对象处理不当。如果用户打开经特殊设计的恶意 Office 文件，可能会导致此漏洞被利用，使攻击者可以在当前用户环境中执行攻击者选择的任意代码。这类攻击情况包括基于邮件的攻击（攻击者向受害者发送包含恶意附件的邮件）或基于 Web 的攻击（用户下载并打开恶意 Office 文件）。

多个 CVE - Microsoft Office SharePoint XSS 漏洞

在 Microsoft Office Sharepoint 中发现了多个漏洞，攻击者可能会利用些个漏洞执行跨站点脚本 (XSS) 攻击。出现这两个漏洞是因为 Sharepoint Server 未正确清理用户的特定 Web 请求。成功利用这些漏洞的攻击者可以在当前用户环境下执行脚本，读取攻击者原本无权查看的内容，或代表受影响的用户执行操作。

以下 CVE 可以反映这些漏洞：

- CVE-2017-11775
- CVE-2017-11777
- CVE-2017-11820

CVE-2017-11776 - Microsoft Outlook 信息泄露漏洞

在 Microsoft Outlook 中发现了一个信息泄露漏洞，可能会导致敏感信息被泄露给第三方。出现此漏洞是因为 Outlook 无法建立安全连接。利用此漏洞的攻击者可以获取用户的邮件内容。

CVE-2017-11774 - Microsoft Outlook 安全功能绕过漏洞

在 Microsoft Outlook 中发现了一个安全功能绕过漏洞，攻击者可能会利用此漏洞执行任意命令。出现这个漏洞是因为 Office 对内存中的对象处理不当。如果用户打开经特殊设计的文档文件，则可能会被攻击者利用发起攻击。此漏洞可能会被利用的一种情况是文件共享攻击，在此类攻击中，攻击者为用户提供一个文件并通过社会工程方式诱使其打开。

CVE-2017-11772 - Microsoft Search 信息泄露漏洞

在 Windows Search 中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞获取可用于进一步攻击受影响系统的信息。出现此漏洞是因为 Windows Search 对内存中的对象处理不当。如果某个经过身份验证的用户向 Windows Search 服务发送经特殊设计的消息，则此漏洞可能会被利用。或者，某个未经身份验证的攻击者可能会在采用 SMB 连接的企业环境中远程利用此漏洞。

CVE-2017-11823 - Microsoft Windows 安全功能绕过漏洞

在 Device Guard 中发现了一个漏洞，攻击者可利用此漏洞绕过安全控制并向 Windows Powershell 会话注入恶意代码。此漏洞是由于 Device Guard 实施代码完整性策略的方式导致的。具有本地计算机访问权限的攻击者可以向代码完整性策略信任的脚本中注入恶意代码。这样一来，注入的代码将按照与脚本相同的信任级别运行，绕过代码完整性策略控制。

CVE-2017-11786 - Skype for Business 权限提升漏洞

在 Skype for Business 中发现了一个权限提升漏洞，经过身份验证的攻击者可能会利用此漏洞冒充用户。出现此漏洞是因为 Skype for Business 对特定身份验证请求处理不当。如果攻击者在设置经特殊设计的个人资料照片后发起即时消息会话，则可利用此漏洞并窃取可在其他环境下重复使用的身份验证散列值。成功利用此漏洞的攻击者可以执行用户有权执行的操作，从而导致权限提升等各种后果。

CVE-2017-11769 - TRIE 远程代码执行漏洞

在 Windows 中发现了一个任意代码执行漏洞，攻击者可能会利用此漏洞在当前用户环境中执行代码。出现此漏洞是因为某些 Windows 组件对加载 DLL 文件的方式处理不当。成功利用此漏洞的攻击者可以在当前用户环境下执行操作或执行命令。

CVE-2017-8689、CVE-2017-8694 - Win32k 权限提升漏洞

在 Windows 内核模式驱动程序中发现了两个漏洞，它们可能会引发权限提升攻击。出现这些漏洞是因为对内存中的对象处理不当。成功利用这些漏洞会使攻击者在目标系统上获得管理员权限。如果用户运行经特殊设计的、利用此漏洞的可执行文件，则可以利用此漏洞在受影响的系统上以管理员身份执行操作。

CVE-2017-11783 - Windows 权限提升漏洞

在 Windows 中发现了一个权限提升漏洞，经过身份验证的攻击者可能会利用此漏洞将其权限提升为管理员权限。出现此漏洞是因为 Windows 未正确处理对高级本地过程调用 (ALPC) 的调用。如果用户创建经特殊设计的应用，并在受影响的系统上执行，则可以利用此漏洞。

CVE-2017-11816 - Windows GDI 信息泄露漏洞

在 Microsoft Windows 图形设备接口 (GDI) 中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞获取可用于进一步攻击受影响系统的信息。出现此漏洞是因为 GDI 对内存中的对象处理不当。如果某个经过身份验证的用户要启动旨在利用此漏洞的经特殊设计的可执行文件，则此漏洞可能会被利用。

CVE-2017-11824 - Windows 图形组件权限提升漏洞

在 Microsoft Windows 图形组件中发现了一个权限提升漏洞，攻击者可能会利用此漏洞将其权限提升为管理员权限。出现此漏洞是因为图形组件对内存中的对象处理不当。如果某个经过身份验证的用户要启动旨在利用此漏洞的经特殊设计的可执行文件，则此漏洞可能会被利用。

CVE-2017-11817 - Windows 信息泄露漏洞

在 Windows 内核中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞获取可用于进一步攻击受影响系统的信息。出现此漏洞是因为内核未正确初始化内存中的对象。如果某个经过身份验证的用户要启动旨在利用此漏洞的经特殊设计的可执行文件，则此漏洞可能会被利用。

CVE-2017-11784、CVE-2017-11785 - Windows 内核信息泄露漏洞

在 Windows 内核中发现了两个信息泄露漏洞，攻击者可能会利用这些漏洞获取内存地址并绕过内核地址空间布局随机化 (KASLR)。如果某个经过身份验证的用户要启动旨在利用这些漏洞的经特殊设计的可执行文件，则这些漏洞可能会被利用。

CVE-2017-11765、CVE-2017-11814 - Windows 信息泄露漏洞

在 Windows 内核中发现了两个信息泄露漏洞，攻击者可能会利用这些漏洞获取可用于进一步攻击受影响系统的信息。出现这些漏洞是因为内核未正确初始化内存中的对象。如果某个经过身份验证的用户要启动旨在利用这些漏洞的经特殊设计的可执行文件，则这些漏洞可能会被利用。

CVE-2017-8715 - Windows 安全功能绕过漏洞

在 Device Guard 中发现了一个漏洞，攻击者可能会利用此漏洞绕过安全控制并向 Windows Powershell 会话注入恶意代码。此漏洞是由于 Device Guard 实施代码完整性策略的方式导致的。具有本地计算机访问权限的攻击者可以向代码完整性策略信任的脚本中注入恶意代码。这样一来，注入的代码将按照与脚本相同的信任级别运行，绕过代码完整性策略控制。

CVE-2017-11781 - Windows SMB 拒绝服务漏洞

在 Microsoft SMB 中发现了一个拒绝服务漏洞，攻击者可能会利用此漏洞使受影响的主机出现故障。出现此漏洞是因为 SMB 对某些请求处理不当。如果攻击者向易受攻击的服务器发送经特殊设计的请求，则可利用此漏洞并为用户创建拒绝服务条件。

CVE-2017-11782 - Windows SMB 权限提升漏洞

在默认的 Windows SMB 服务器配置中发现了一个权限提升漏洞，匿名用户可能会利用此漏洞访问某些命名管道。这些命名管道可以用来向通过命名管道接受请求的服务发送经特殊设计的请求。如果攻击者能够向受影响的 SMB 服务器发送 SMB 消息，则可以利用此漏洞。

CVE-2017-11815 - Windows SMB 信息泄露漏洞

在 Windows SMB 中发现了一个信息泄露漏洞，攻击者可能会利用此漏洞访问原本无权访问的文件。出现此漏洞是因为 SMB 服务器对某些请求处理不当。如果攻击者经过身份验证，能够访问 SMB 服务器并向其发送 SMB 消息，则可以利用此漏洞。

CVE-2017-11780 - Windows SMB 远程代码执行漏洞

在 Microsoft Server Message Block 1.0 (SMBv1) 中发现了一个远程代码执行漏洞，攻击者可能会利用此漏洞攻击 SMBv1 服务器。出现此漏洞是因为 SMBv1 服务器对某些请求的处理方式不当。未经身份验证的攻击者可以向受影响的服务器发送经特殊设计的请求，从而利用此漏洞。

CVE-2017-11818 - Windows Storage 安全功能绕过漏洞

在 Microsoft Windows Storage 中发现了一个安全功能绕过漏洞，具有特定完整性级别的应用可能会利用此漏洞在其他级别执行代码。出现此漏洞是因为 Windows 未正确验证完整性级别检查。

CVE-2017-8703 - 适用于 Linux 的 Windows 子系统拒绝服务漏洞

在适用于 Linux 的 Windows 子系统 (WSL) 中发现了一个拒绝服务漏洞。出现此漏洞是因为 WSL 对内存中的对象处理不当。如果攻击者创建经特殊设计的应用，并在受影响的系统上执行，则可以利用此漏洞。

CVE-2017-11829 - Windows 更新传递优化权限提升漏洞

在 Windows 更新传递优化中发现了一个权限提升漏洞，攻击者可能会利用此漏洞覆盖高于其所拥有权限的文件。出现此漏洞是因为 Windows 更新传递优化对文件共享权限执行不当。如果攻击者能够登录系统并创建一个传递优化作业，则可以利用此漏洞。

防护

为了应对发现的这些漏洞，Talos 发布了以下 Snort 规则来检测利用这些漏洞的尝试。请注意，Talos 未来可能会发布更多规则，当前规则会根据未来得到的更多信息而有所变更。Firepower 客户应更新 SRU，使用最新的规则集更新。打开源 Snort 用户规则集客户可以在 Snort.org 上下载出售的最新规则包，保持最新状态。

Snort 规则：

- 44333-44334
- 44508-44519
- 44526-44529
- 44532-44533

发布者：ALEXANDER CHIU；发布时间：4:25 PM
标签：MICROSOFT、星期二补丁、SNORT 规则