2017 年 11 月 14 日，星期二

# Microsoft 星期二补丁 - 2017 年 11 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。本月发布的报告可修复 53 个新漏洞，其中 19 个为严重等级漏洞，31 个为重要等级漏洞，3 个为中等等级漏洞。这些漏洞对 Microsoft Edge、Internet Explorer、Microsoft Scripting Engine 等有影响。

此外，Microsoft 还发布了 Adobe Reader 的更新，解决了 CVE-2017-16367/TALOS-2017-0356 - Adobe Acrobat Reader DC PDF 结构化层级 ActualText 结构元素代码执行漏洞，该漏洞最初由思科 Talos 团队的 Aleksandar Nikolic 发现。此漏洞表现为 PDF 解析功能在对包含标记结构元素的文档进行解析时存在类型混淆漏洞。专门用于触发此漏洞的特制 PDF 文档可以导致对堆进行越界访问，从而允许攻击者执行任意代码。有关此漏洞的更多详细信息，请参见此处。

## 评为严重等级的漏洞

以下是 Microsoft 评为“严重”等级的漏洞：

- CVE-2017-11836 - 脚本引擎内存损坏漏洞
- CVE-2017-11837 - 脚本引擎内存损坏漏洞
- CVE-2017-11838 - 脚本引擎内存损坏漏洞
- CVE-2017-11839 - 脚本引擎内存损坏漏洞
- CVE-2017-11840 - 脚本引擎内存损坏漏洞
- CVE-2017-11841 - 脚本引擎内存损坏漏洞
- CVE-2017-11843 - 脚本引擎内存损坏漏洞
- CVE-2017-11845 - Microsoft Edge 内存损坏漏洞
- CVE-2017-11846 - 脚本引擎内存损坏漏洞
- CVE-2017-11855 - Internet Explorer 内存损坏漏洞
- CVE-2017-11856 - Internet Explorer 内存损坏漏洞
- CVE-2017-11858 - 脚本引擎内存损坏漏洞
- CVE-2017-11861 - 脚本引擎内存损坏漏洞
- CVE-2017-11862 - 脚本引擎内存损坏漏洞
- CVE-2017-11866 - 脚本引擎内存损坏漏洞

- CVE-2017-11869 - 脚本引擎内存损坏漏洞
- CVE-2017-11870 - 脚本引擎内存损坏漏洞
- CVE-2017-11871 - 脚本引擎内存损坏漏洞
- CVE-2017-11873 - 脚本引擎内存损坏漏洞

## 多个 CVE - 脚本引擎内存损坏漏洞

在 Microsoft Edge 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 Microsoft Edge 对内存中的对象处理不当。这些漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用这些漏洞的恶意网页。成功利用这些漏洞的攻击者可在当前用户环境下执行代码。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11836
- CVE-2017-11839
- CVE-2017-11840
- CVE-2017-11841
- CVE-2017-11861
- CVE-2017-11862
- CVE-2017-11866
- CVE-2017-11870
- CVE-2017-11871
- CVE-2017-11873

## 多个 CVE - 脚本引擎内存损坏漏洞

在 Microsoft 浏览器中发现了多个影响脚本引擎的远程代码执行漏洞。出现这些漏洞是因为脚本引擎对内存中的对象处理不当。成功利用这些漏洞的攻击者可在当前用户环境下执行任意代码。这些漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图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-2017-11837
- CVE-2017-11838
- CVE-2017-11843
- CVE-2017-11846
- CVE-2017-11858

## CVE-2017-11845 - Microsoft Edge 内存损坏漏洞

发现了一个影响 Microsoft Edge 的远程代码漏洞。该漏洞与 Microsoft Edge 访问内存中对象的方式有关。成功利用此漏洞的攻击者可以使用与当前用户相同的访问权限执行任意代码。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页，或者使用诱使其打开的恶意电子邮件附件。

## 多个 CVE - Internet Explorer 内存损坏漏洞

发现了两个影响 Internet Explorer 的远程代码漏洞。这些漏洞与 Internet Explorer 访问内存中对象的方式有关。成功利用这些漏洞的攻击者可以使用与当前用户相同的访问权限执行任意代码。这些漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页，或者使用诱使其打开的恶意电子邮件附件。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11855
- CVE-2017-11856

## CVE-2017-11869 - 脚本引擎内存损坏漏洞

在 Internet Explorer 的脚本引擎中发现了一个漏洞，攻击者可能会利用这些漏洞远程执行任意代码。出现此漏洞是因为 Internet Explorer 不正确地访问内存中的对象。这些漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用这些漏洞的恶意网页。成功利用这些漏洞的攻击者可在当前用户环境下执行代码。

## 评为重要等级的漏洞

以下是 Microsoft 评为“重要”等级的漏洞：

- CVE-2017-11768 - Windows Media Player 信息泄露漏洞
- CVE-2017-11770 - ASP.NET Core 拒绝服务漏洞
- CVE-2017-11788 - Windows Search 拒绝服务漏洞
- CVE-2017-11791 - 脚本引擎信息泄露漏洞
- CVE-2017-11803 - Microsoft Edge 信息泄露漏洞
- CVE-2017-11827 - Microsoft 浏览器内存损坏漏洞
- CVE-2017-11830 - Device Guard 安全功能绕过漏洞
- CVE-2017-11831 - Windows 信息泄露漏洞
- CVE-2017-11832 - Windows EOT 字体引擎信息泄露漏洞
- CVE-2017-11833 - Microsoft Edge 信息泄露漏洞
- CVE-2017-11834 - 脚本引擎信息泄露漏洞
- CVE-2017-11835 - Windows EOT 字体引擎信息泄露漏洞
- CVE-2017-11842 - Windows 内核信息泄露漏洞
- CVE-2017-11844 - Microsoft Edge 信息泄露漏洞
- CVE-2017-11847 - Windows 内核权限提升漏洞
- CVE-2017-11849 - Windows 内核信息泄露漏洞
- CVE-2017-11850 - Microsoft 图形组件信息泄露漏洞
- CVE-2017-11851 - Windows 内核信息泄露漏洞
- CVE-2017-11852 - Windows GDI 信息泄露漏洞
- CVE-2017-11853 - Windows 内核信息泄露漏洞
- CVE-2017-11854 - Microsoft Word 内存损坏漏洞
- CVE-2017-11863 - Microsoft Edge 安全功能绕过漏洞
- CVE-2017-11872 - Microsoft Edge 安全功能绕过漏洞
- CVE-2017-11874 - Microsoft Edge 安全功能绕过漏洞
- CVE-2017-11877 - Microsoft Excel 安全功能绕过漏洞
- CVE-2017-11878 - Microsoft Excel 内存损坏漏洞
- CVE-2017-11879 - ASP.NET Core 权限提升漏洞
- CVE-2017-11880 - Windows 信息泄露漏洞
- CVE-2017-11882 - Microsoft Office 内存损坏漏洞
- CVE-2017-11884 - Microsoft Office 内存损坏漏洞

## CVE-2017-11768 - Windows Media Player 信息泄露漏洞

发现了影响 Windows Media Player 的信息泄漏漏洞。出现此漏洞是因为 Windows Media Player 不当地泄露了文件信息。要利用此漏洞，攻击者需要通过受影响系统的身份验证，并执行专门用于利用此漏洞的程序。成功利用此漏洞的攻击者可以枚举存储在受影响系统上的文件。

## 多个 CVE - ASP.NET Core 拒绝服务漏洞

发现了影响 ASP.NET Core 的多个拒绝服务漏洞。出现这些漏洞是因为 .NET Core 对 Web 请求处理不当。未经身份验证的攻击者可以远程利用这些漏洞。成功利用此漏洞可能造成拒绝服务情况。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11770 - ASP.NET Core 拒绝服务漏洞
- CVE-2017-11883 - ASP.NET Core 拒绝服务漏洞

## CVE-2017-11788 - Windows Search 拒绝服务漏洞

发现了一个影响 Windows Search 的拒绝服务漏洞。出现此漏洞是因为 Windows Search 对内存中的对象处理不当。攻击者可以通过向 Windows Search 服务发送特制消息来利用此漏洞。此外, 未经身份验证的远程攻击者还可以通过服务器消息块 (SMB) 协议利用此漏洞。成功利用此漏洞可能导致受影响的系统出现拒绝服务情况。

## CVE-2017-11791 - 脚本引擎信息泄露漏洞

发现了一个影响 Microsoft 浏览器的信息泄露漏洞。出现此漏洞是因为 Windows 浏览器对内存中的对象处理不当。攻击者可以利用此漏洞获取可用于对受影响系统进行后续攻击的信息。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页。

## 多个 CVE - Windows Edge 信息泄露漏洞

发现了两个影响 Microsoft Edge 的信息泄露漏洞。出现这些漏洞是因为 Microsoft Edge 对内存中的对象处理不当。攻击者可以利用这些漏洞获取可用于对受影响系统进行后续攻击的信息。这些漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11803
- CVE-2017-11844

## CVE-2017-11827 - Microsoft 浏览器内存损坏漏洞

发现了一个影响 Microsoft 浏览器的远程代码执行漏洞。出现此漏洞是因为 Microsoft 浏览器对内存中的对象处理不当。成功利用此漏洞的攻击者可通过与当前用户相同的权限执行任意代码。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页，或者诱使用户打开恶意电子邮件附件。

## CVE-2017-11830 - Device Guard 安全功能绕过漏洞

发现了一个影响 Device Guard 的安全功能绕过漏洞。出现此漏洞是因为 Device Guard 错误地验证了不受信任的文件。成功利用此漏洞的攻击者可以将未签名的文件充当签名文件，从而使攻击者可在受影响的系统上执行恶意文件。

## 多个 CVE - Windows 信息泄露漏洞

发现了多个影响 Windows 内核的信息泄露漏洞。出现这些漏洞是由于 Windows 内核无法正确初始化内存地址。攻击者可以利用这些漏洞获取可用于对受影响系统进行后续攻击的信息。要利用这些漏洞，攻击者需要通过受影响设备的身份验证，并执行专门用于利用此漏洞的应用程序。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11831
- CVE-2017-11880

## 多个 CVE - Windows EOT 字体引擎信息泄露漏洞

发现了两个影响 Microsoft Windows Embedded OpenType (EOT) 的信息泄露漏洞。出现这些漏洞是因为字体引擎对嵌入字体解析不当。成功利用这些漏洞的攻击者可以获取可用于对受影响系统进行后续攻击的信息。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11832
- CVE-2017-11835

## CVE-2017-11833 - Microsoft Edge 信息泄露漏洞

发现了一个影响 Microsoft Edge 的信息泄露漏洞。出现此漏洞是因为 Microsoft Edge 对跨网域请求处理不当。攻击者可以利用此漏洞来确定受影响浏览器中的网页来源。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页。

## CVE-2017-11834 - 脚本引擎信息泄露漏洞

发现了一个影响 Internet Explorer 的信息泄露漏洞。出现此漏洞是因为 Internet Explorer 中的脚本引擎对内存中的对象处理不当。攻击者可以利用此漏洞获取可用于进行额外攻击的信息。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页。

## 多个 CVE - Windows 内核信息泄露漏洞

发现了多个影响 Microsoft 内核模式驱动程序的信息泄露漏洞。出现这些漏洞是由于 Windows 内核无法正确初始化内存地址。攻击者可以利用这些漏洞获取可用于对受影响系统进行进一步后续攻击的信息。利用这些漏洞需要攻击者登录并执行专门用来利用它们的程序。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11842
- CVE-2017-11849
- CVE-2017-11853

## CVE-2017-11847 - Windows 内核权限提升漏洞

发现了一个影响 Windows 内核的权限升级漏洞。出现此漏洞是因为 Windows 内核对内存中的对象处理不当。要成功利用此漏洞，攻击者需要登录一个系统并执行专门用来利用此漏洞的程序，这使攻击者可以在内核内存中运行任意代码。

## CVE-2017-11850 - Microsoft 图形组件信息泄露漏洞

发现了一个影响 Microsoft 图形组件的信息泄露漏洞。出现此漏洞是因为 Windows GDI 组件泄露了内核内存的地址。攻击者可以利用此漏洞获取可用于对受影响系统进行额外攻击的信息。要成功利用此漏洞，攻击者需要登录一个系统并执行专门用来利用此漏洞的程序。

## CVE-2017-11851 - Windows 内核信息泄露漏洞

发现了一个影响 Microsoft 图形组件的信息泄露漏洞。出现此漏洞是因为 Windows GDI 组件泄露了内核内存的地址。攻击者可以利用此漏洞获取可用于对受影响系统进行额外攻击的信息。要成功利用此漏洞，攻击者需要登录一个系统并执行专门用来利用此漏洞的程序。

## CVE-2017-11852 - Windows GDI 信息泄露漏洞

发现了一个影响 Microsoft 图形组件的信息泄露漏洞。出现此漏洞是因为 Windows GDI 组件泄露了内核内存的地址。攻击者可以利用此漏洞获取可用于对受影响系统进行额外攻击的信息。要成功利用此漏洞，攻击者需要登录一个系统并执行专门用来利用此漏洞的程序。

## CVE-2017-11854 - Microsoft Word 内存损坏漏洞

发现了一个影响 Microsoft Office 的远程代码执行漏洞。出现此漏洞是因为 Microsoft Office 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。要利用此漏洞，攻击者需要创建一个特制文件，并诱使用户在受影响的 Microsoft Office 版本中打开它。

## CVE-2017-11863 - Microsoft Edge 安全功能绕过漏洞

在 Microsoft Edge 中发现了一个安全功能绕过漏洞，它使攻击者可在用户不知情或未同意的情况下加载包含恶意内容的页面。出现此漏洞是因为 Edge 内容安全策略对某些特制文档的验证不当。攻击者可以通过诱使用户导航到恶意页面或将恶意内容（如广告）插入到页面中，从而绕过内容安全策略来利用此漏洞。

## CVE-2017-11872 - Microsoft Edge 安全功能绕过漏洞

在 Microsoft Edge 中发现了一个安全功能绕过漏洞，它可以让攻击者绕过跨域资源共享限制。出现此漏洞是因为 Edge 对重定向请求处理不当并遵从本应忽略的重定向请求。攻击者可以通过创建意图利用此漏洞的特制网页并诱使用户访问此网页来利用此漏洞。此外，攻击者也可以通过易受攻击或受损的网页利用此漏洞。

## CVE-2017-11874 - Microsoft Edge 安全功能绕过漏洞

在 Microsoft Edge 中发现了一个安全功能绕过漏洞，它可以让攻击者绕过控制流防护。出现此漏洞是因为 Edge Just-In-Time 编译器对已编译代码中的内存操作处理不当。攻击者可以通过创建意图利用此漏洞的特制网页并诱使用户访问此网页来利用此漏洞。

## CVE-2017-11877 - Microsoft Excel 安全功能绕过漏洞

发现了一个影响 Microsoft Office 的安全功能绕过漏洞。此漏洞与 Microsoft Office 无法在 Excel 文档上执行宏设置有关。利用此漏洞不会导致代码执行，并且攻击者需要创建一个可在受影响的 Microsoft Excel 版本中打开的特制文件。

## CVE-2017-11878 - Microsoft Excel 内存损坏漏洞

发现了一个影响 Microsoft Office 的远程代码执行漏洞。此漏洞与 Microsoft Office 对内存中的对象处理不当有关。成功利用此漏洞的攻击者可以在当前用户的环境中执行任意代码。要利用此漏洞，攻击者需要创建一个可在受影响的 Microsoft Office 版本中打开的特制文件。

## CVE-2017-11879 - ASP.NET Core 权限提升漏洞

发现了一个影响 ASP.NET Core 的打开重定向漏洞。利用此漏洞会导致权限提升。要利用此漏洞，攻击者需要创建一个特制的 URL，用于将受害者的浏览器会话重定向到恶意网站并获取登录会话信息。

## 多个 CVE - Microsoft Office 内存损坏漏洞

发现了多个影响 Microsoft Office 的远程代码执行漏洞。这些漏洞与 Microsoft Office 对内存中的对象处理不当有关。成功利用这些漏洞的攻击者可以在当前用户的环境中执行任意代码。要利用此漏洞，攻击者需要创建一个可在受影响的 Microsoft Office 版本中打开的特制文件。

以下是与这些漏洞有关的 CVE 列表：

- CVE-2017-11882
- CVE-2017-11884

## 评为中等等级的漏洞

以下是 Microsoft 评为“中等”等级的漏洞：

- CVE-2017-11848 - Internet Explorer 信息泄露漏洞
- CVE-2017-11876 - Microsoft Project Server 权限提升漏洞
- CVE-2017-8700 - ASP.NET Core 信息泄露漏洞

### CVE-2017-11848 - Internet Explorer 信息泄露漏洞

发现了一个影响 Internet Explorer 的信息泄露漏洞。出现此漏洞是因为 Internet Explorer 处理网页内容的方式不当。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页。成功利用此漏洞的攻击者可以检测到离开恶意网页的用户的导航。

### CVE-2017-11876 - Microsoft Project Server 权限提升漏洞

发现了一个影响 Microsoft Project 的权限提升漏洞。它与 Microsoft Project Server 管理用户会话的方式不当有关。受害者必须登录到目标站点，才会使此漏洞被利用。此漏洞可能被利用的情况包括基于 Web 的攻击，在此类攻击中，用户会导航至意图利用此漏洞的恶意网页。成功利用此漏洞的攻击者可以从 Web 应用程序内部访问其无权访问的内容或者伪装成真正的用户。它也可以让攻击者向受害者的浏览器中注入恶意内容。

### CVE-2017-8700 - ASP.NET Core 信息泄露漏洞

发现了一个影响 ASP.net Core 的信息泄露漏洞。此漏洞可以让攻击者绕过跨域资源共享 (CORS) 配置。成功利用此漏洞的攻击者可以从 Web 应用程序内部访问其无权访问的内容。

## 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：

- 43120-43121
- 44809-44834
- 44838-44839
- 44843-44846

如需了解 Talos 披露的其他漏洞，请访问我们的漏洞报告门户：
http://www.talosintelligence.com/vulnerability-reports/

如需查看我们的漏洞披露政策，请访问此网站：

http://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html

发布者：Edmund Brumaghin；发布时间 2:54 PM
标签：修补程序星期二、安全更新、漏洞