2017 年 7 月 11 日，星期二

Microsoft 星期二补丁 - 2017 年 7 月

今天，Microsoft 发布了旨在修复漏洞的一系列月度安全更新。本月发布的安全更新可修复 54 个漏洞，其中 19 个为严重等级漏洞，32 个为重要等级漏洞，3 个为中等等级漏洞。受影响的产品包括 Edge、.NET Framework、Internet Explorer、Office 和 Windows。

评为严重等级的漏洞

CVE-2017-8463

一种远程代码执行漏洞，与重命名操作期间 Windows Explorer 处理可执行文件和共享的方式有关。成功利用此漏洞的攻击者可以运行任意代码，非管理员用户受到的影响相对较小。攻击者可通过恶意共享文件夹和带有可执行文件扩展名的恶意软件触发此漏洞。

CVE-2017-8584

HoloLens 未正确处理内存对象时出现的一种远程代码执行漏洞。成功利用此漏洞的攻击者可以控制受影响的系统，并且之后可以安装程序；查看、更改或删除数据；或创建具有完整用户权限的新帐户。要利用此漏洞，攻击者需要发送经特殊设计的 WiFi 数据包。

CVE-2017-8589

一种在 Windows Search 未正确处理内存中的对象时出现的远程代码执行漏洞。攻击者可通过向 Windows Search 服务发送经特殊设计 SMB 消息对漏洞加以利用。

CVE-2017-8594

一种使用 Internet Explorer 时出现的远程代码执行漏洞。通过该漏洞，攻击者可以利用当前用户权限执行任意代码，进而导致内存损坏。如果当前用户是使用管理用户权限登录，那么攻击者可以控制受影响的系统，并且之后可以安装程序；查看、更改或删除数据；或创建具有完整用户权限的新帐户。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8595/CVE-2017-8596/CVE-2017-8617

一种存在于 Microsoft Edge 中的远程代码执行漏洞。通过该漏洞，攻击者可以使用当前用户权限执行任意代码，进而损坏内存。如果当前用户是使用管理用户权限登录，那么攻击者可以控制受影响的系统，并且之后可以安装程序；查看、更改或删除数据；或创建具有完整用户权限的新帐户。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。此外，攻击者可在托管浏览器渲染引擎的应用或 Microsoft Office 文档中嵌入标记为“安全初始化”的 ActiveX 控件。

CVE-2017-8598

一种在 Microsoft Edge 未正确处理内存对象时出现的远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户查看经特殊设计的网站，或通过应用或 Microsoft Office 文档中标记为“安全初始化”的 ActiveX 控件发动针对此漏洞的攻击。

CVE-2017-8601

Microsoft 浏览器的 Chakra JavaScript 引擎在未正确处理内存对象时出现的一种远程代码执行漏洞。攻击者可通过经特殊设计的网站或标记为“安全初始化”的 ActiveX 插件来利用该漏洞，从而对受影响的系统进行全面控制。

CVE-2017-8603

一种存在于 Microsoft Edge 中的远程代码执行漏洞，与引擎处理内存对象的方式有关。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8604

一种在 Microsoft Edge 未正确处理内存对象时出现的远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户查看经特殊设计的网站，或通过应用或 Microsoft Office 文档中标记为“安全初始化”的 ActiveX 控件发动针对此漏洞的攻击。

CVE-2017-8605

一种在 Microsoft Edge 未正确处理内存对象时出现的远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户查看经特殊设计的网站，或通过应用或 Microsoft Office 文档中标记为“安全初始化”的 ActiveX 控件发动针对此漏洞的攻击。

CVE-2017-8606/CVE-2017-8607/CVE-2017-8608/CVE-2017-8609

Microsoft 浏览器 JavaScript 引擎在未正确处理内存中的对象时出现的一种远程代码执行漏洞。攻击者可以通过让用户查看经特殊设计的网站来利用该漏洞，从而获得与当前用户相同的用户权限。

CVE-2017-8610

一种在 Microsoft Edge 未正确处理内存对象时出现的远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过让用户查看经特殊设计的网站或通过应用或 Microsoft Office 文档中标记为“安全初始化”的 ActiveX 控件对漏洞加以利用。

CVE-2017-8618

一种远程代码执行漏洞，存在于 Internet Explorer 处理内存对象时渲染的 VBScript 引擎中。攻击者可以通过让用户查看经特殊设计的网站来利用该漏洞，从而获得与当前用户相同的用户权限。

CVE-2017-8619

在 Microsoft Edge 浏览器错误访问内存中的对象时出现的两种远程代码执行漏洞。这种漏洞会造成内存损坏，这样攻击者可执行任意代码。攻击者可通过让用户访问经特殊设计的网站对漏洞加以利用。

评为中等等级的漏洞

CVE-2017-0170

一种信息披露漏洞，当 Windows 性能监测控制台未正确解析 XML 输入时，在此控制台上出现。成功利用此漏洞的攻击者可以通过 XML 外部实体 (XXE) 读取任意文件。为了利用此漏洞，攻击者可能会创建经特殊设计的 XML 数据并诱使经过身份验证的用户创建数据收集器集并导入此文件。要创建数据收集器集，用户必须是性能日志用户或本地管理员组的成员。

CVE-2017-8611

一种在 Microsoft Edge 未正确解析 HTTP 内容时出现的欺骗漏洞。攻击者可使用经特殊设计的网站对恶意内容进行伪装，或者利用该网站作为“枢纽”，发动利用其他漏洞的联合攻击。

CVE-2017-8621

Microsoft Exchange 中存在的一种可能会导致欺骗的开放重定向漏洞。为了利用此漏洞，攻击者可能会发送经特殊设计的 URL，当经过身份验证的 Exchange 用户点击该链接时，经过身份验证的用户的浏览器会话可能会被重定向到刻意模拟合法网站的恶意站点。如此一来，该攻击者便可以欺骗用户，并且可能会获取敏感信息，例如用户凭证。

评为重要等级的漏洞

CVE-2017-0243

一种远程代码执行漏洞，在 Microsoft Office 软件未正确处理内存对象时出现在此软件中。成功利用此漏洞的攻击者能够以当前用户的权限执行操作。攻击者可通过诱使用户打开经特殊设计的文件对漏洞加以利用。

CVE-2017-8467

一种特权提升漏洞，在 Windows 图形组件未能正确处理内存对象时出现于 Windows 中。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-8486

一种信息披露漏洞，在 Win32k 未能正确处理内存对象时出现于 Microsoft Windows 中。经过身份验证的攻击者可通过执行经特殊设计的应用来触发这些漏洞。

CVE-2017-8495

一种安全功能绕过漏洞，当 Kerberos 无法防止在票证交换期间篡改 SNAME 时，Microsoft Windows 中会出现此漏洞。针对此漏洞发动的攻击成功后，攻击者可绕过身份验证扩展保护。

CVE-2017-8501 / CVE-2017-8502

一种在 Microsoft Office 未正确处理内存中的对象时出现的远程代码执行漏洞。攻击者在用户打开经特殊设计的文件时对漏洞加以利用。此文件可以通过电子邮件送达或托管于网站上。

CVE-2017-8556

一种特权提升漏洞，在 Windows 图形组件未能正确处理内存对象时出现于 Windows 中。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-8557

一种信息披露漏洞，在 Windows 系统信息控制台未正确解析 XML 输入时出现在此控制台上。成功利用此漏洞的攻击者可以通过 XML 外部实体 (XXE) 读取任意文件。为了利用此漏洞，攻击者可能会创建经特殊设计的 XML 数据。

CVE-2017-8559 / CVE-2017-8560

Microsoft Exchange Outlook Web Access (OWA) 未能正确处理 Web 请求时出现的一种特权提升漏洞。经过身份验证的攻击者可通过发送经特殊设计的请求对漏洞加以利用。

CVE-2017-8561

一种在 Windows 内核未正确处理内存中的对象时出现的权限提升漏洞。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-8562

一种特权提升漏洞，当 Windows 未正确处理高级本地过程调用功能 (ALPC) 的调用时出现。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-8563

一种特权提升漏洞，当 Kerberos 回退到使用 NT LAN Manager (NTLM) 身份验证协议作为默认身份验证协议时出现在 Microsoft Windows 中。本地攻击者可通过执行经特殊设计的应用将恶意流量发送到域控制器来利用此漏洞。

CVE-2017-8564

一种在 Windows 内核未正确处理内存中的对象时出现的信息披露漏洞。本地攻击者可通过执行经特殊设计的应用来利用此漏洞，让攻击者能够绕过内核地址空间布局随机化 (KASLR) 检索信息。

CVE-2017-8565

一种远程代码执行漏洞，在 PSObject 隐藏 CIM 实例时出现在 PowerShell 中。成功利用该漏洞的攻击者能够在易受攻击的系统上执行恶意代码。

CVE-2017-8566

一种特权提升漏洞，在 Windows 输入法编辑器 (IME) 以 DCOM 类的方式不正确地处理参数时出现在 IME 中。无论启用哪种语言/IME，系统上都安装了 DCOM 服务器，攻击者可以实例化 DCOM 类并对系统加以利用，即使 IME 未启用。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-8569

一种特权提升漏洞，在 Microsoft SharePoint 服务器未正确清理经特殊设计的 Web 请求时出现在该服务器上。经过身份验证的网络攻击者可通过向受影响的 SharePoint 服务器发送经特殊设计的要求来利用此漏洞。如果攻击成功，攻击者可在受影响的系统上执行跨站点脚本攻击并使用当前用户的权限运行脚本。这使得攻击者可以阅读他们原本无权阅读的内容，使用受害者的身份代表用户在 SharePoint 站点上执行操作（如更改权限和删除内容），以及在用户的浏览器中注入恶意内容。

CVE-2017-8570

一种远程代码执行漏洞，在 Microsoft Office 软件未正确处理内存对象时出现在此软件中。成功利用此漏洞的攻击者能够以当前用户的权限执行操作。攻击者可通过诱使用户打开经特殊设计的文件对漏洞加以利用。

CVE-2017-8573/CVE-2017-8574/CVE-2017-8577/CVE-2017-8578/CVE-2017-8580

一种存在于 Microsoft 图形组件中的特权提升漏洞。成功利用此漏洞的攻击者可以在内核模式下运行任意代码。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

CVE-2017-8581

Windows 未正确处理内存对象时出现的一种特权提升漏洞。经过身份验证并成功利用此漏洞的攻击者能够以更高的权限运行程序。

CVE-2017-8582

一种信息披露漏洞，在 HTTP.sys 服务器应用组件未正确处理内存对象时出现。未经身份验证的远程攻击者可通过向服务器应用发送请求来利用此漏洞。

CVE-2017-8585

一种拒绝服务漏洞，在 Microsoft 公共对象运行时库未正确处理网络请求时出现。未经身份验证的远程攻击者可通过向 NET 应用发送经特殊设计的请求来利用此漏洞。此攻击会导致目标系统出现拒绝服务的情况，并需要重启才能解决。

CVE-2017-8587

一种拒绝服务漏洞，在 Windows 资源管理器试图打开不存在的文件时出现。攻击者利用此漏洞的方式可以是托管一个经特殊设计的网站，并诱使用户浏览此网站上的页面，而页面上包含对不存在的文件的引用，最终导致受害者的系统停止响应。

CVE-2017-8588

一种远程代码执行漏洞，在 Microsoft WordPad 解析经特殊设计的文件时出现。攻击者若要利用此漏洞，需要用户使用受感染版本的 Microsoft WordPad 打开经特殊设计的文件。攻击者可通过邮件向用户发送经特殊设计的文件来利用此漏洞。

CVE-2017-8590

一种存在于 Windows 通用日志文件系统 (CLFS) 中的特权提升漏洞。在本地经过身份验证的攻击者可通过运行经特殊设计的应用来利用此漏洞，进而控制受感染的系统。成功利用此漏洞的攻击者能够以更高的权限运行程序。

CVE-2017-8592

一种安全功能绕过漏洞，在 Microsoft 浏览器未正确处理重定向请求时出现。该漏洞能让 Microsoft 浏览器绕过 CORS 重定向限制，并跟踪本应被忽略的重定向请求。成功利用此漏洞的攻击者可以强制浏览器发送本应限制发往目标网站的数据。

CVE-2017-8599

一种安全功能绕过漏洞，在 Microsoft Edge 未能正确针对出现在其他浏览器窗口的 HTML 要素应用同源策略时出现。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8602

一种在 Microsoft 浏览器未正确解析 HTTP 内容时出现的欺骗漏洞。攻击者可使用经特殊设计的网站对恶意内容进行伪装，或者利用该网站作为“枢纽”，发动利用其他漏洞的联合攻击。

防护

为了响应此次 Microsoft 公告，Talos 发布以下规则来解决这些漏洞。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漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅管理中心或 Snort.org。

Snort 规则：
42753
42755-42756
43460-43463
43465-43466
43469-43474
43490-43493
43521-43522

发布者：WILLIAM LARGENT；发布时间：15:59
标签：防护、MICROSOFT、微软周二补丁日、周二补丁日、SNORT 规则、TALOS