2017 年 3 月 14 日，星期二

Microsoft 星期二补丁 - 2017 年 3 月

继 2 月为数不多的几个星期二补丁之后，今天发布的 3 月已修复漏洞数量剧增：17 个公告包括 140 个不同的漏洞，其中 47 个漏洞被列为“严重”等级。这些严重漏洞影响的软件包括 Internet Explorer、Edge、Hyper-V、Windows PDF 库、Microsoft SMB 服务器，Uniscribe、Microsoft 图形组件、Adobe Flash Player 和 Microsoft Windows。92 个漏洞被列为“重要”等级，除上述软件外还影响到 Active Directory 联合身份验证服务、DirectShow、Internet 信息服务、Microsoft Exchange Server、Microsoft Office、Microsoft XML Core Services、Windows DVD Maker、Windows 内核、Windows 内核模式驱动程序。

列为严重等级的公告

MS17-006、MS17-007、MS17-008、MS17-009、MS17-010、MS17-011、MS17-012、MS17-013 和 MS17-023 被列为“严重”等级。

MS17-006 是本月关于 Internet Explorer 的公告。在 6 个 Internet Explorer 严重漏洞中，有 3 个涉及浏览器处理内存中对象的方式所导致的远程代码执行漏洞。其中一个漏洞 (CVE-2017-0149) 目前已被普遍用于漏洞攻击。2 个严重漏洞与 JScript 和 VBScript 处理内存中对象时的呈现方式相关，攻击者可以利用这两个漏洞执行远程代码。虽然其余的严重漏洞本身不会导致执行代码，但是如果配合代码执行漏洞使用，攻击者却可以利用这些严重漏洞，以比允许的 shoallinauld 高的权限执行代码。另外还有 4 个漏洞被列为“重要”等级，这些漏洞可能会被利用来泄露内存或磁盘中的信息。最后 2 个重要漏洞与错误解析 HTTP 标头相关，攻击者有可能利用这些漏洞将受害者重定向至恶意网站。这 2 个漏洞（CVE-2017-0012 和 CVE-2017-033）也存在于 Edge 中，因此也包括在公告 MS17-007 中。

MS17-007 是关于 Edge 中漏洞的公告，描述了 20 个严重漏洞和 10 个重要漏洞。其中 15 个严重漏洞与脚本引擎处理内存中对象时的呈现方式的问题相关，攻击者有可能利用这些漏洞在受影响的系统上执行任意代码。严重漏洞 CVE-2017-0037 是与 Internet Explorer 共有的漏洞，使攻击者可以通过内存损坏漏洞执行任意代码。另有三个漏洞与 Edge 访问内存中对象的方式相关，同样可被滥用来执行任意代码，其中两个漏洞被列为“严重”等级。一个严重漏洞与 MS Windows PDF 库相关，查看包含带有恶意 PDF 内容的网站时，该漏洞可能导致远程代码执行。此漏洞在 MS17-009 中进行了详细描述。Edge 还有一个独有的内存损坏漏洞 - CVE-2017-0034，攻击者可以利用该漏洞以与用户相同的权限执行任意代码。5 个重要漏洞有可能让攻击者得以发现内存中的信息。有 3 个与错误解析 HTTP 标头相关的漏洞被列为“重要”等级，其中 2 个是与 Internet Explorer 共有的漏洞，MS17-006 中也修复了这两个漏洞。因为对 html 元素错误应用相同来源的策略而导致的漏洞中，有 2 个被列为“重要”等级，一个被列为“中等”等级。最后，有一个脚本引擎内存损坏漏洞被列为“重要”等级，与同一体系中的其他严重漏洞不同。

MS17-008 修复了 Windows Hyper-V 中的 11 个漏洞，其中只有 3 个是严重漏洞。导致其中一个漏洞的原因是服务器上的 Hyper-V 无法正确验证 vSMB 数据包数据。攻击者可以通过虚拟机利用此漏洞在主机上执行任意代码。另外还有一个漏洞也与验证 vSMB 数据包相关，但被列为“重要”等级。两个严重漏洞与主机系统如何验证来宾操作系统上经身份验证的用户的输入相关，攻击者有可能利用这些漏洞在主机上执行任意代码。此公告还包括六个对拒绝服务漏洞的重要修复和一个对内存泄露漏洞的重要修复。

MS17-010 修复了 Windows SMB 服务器中的 6 个漏洞。其中的 5 个严重漏洞有可能被攻击者用来将恶意数据包发送到 SMBv1 服务器，从而导致远程执行代码。而另一个更重要漏洞有可能被攻击者用来通过向 SMBv1 服务器发送恶意数据包的方法泄露服务器中的信息。

Microsoft Uniscribe 是用于呈现 Unicode 字符的一系列服务。MS17-011 修复了 Uniscribe 中的 29 个漏洞，其中 8 个漏洞被列为“严重”等级，其余漏洞被列为“重要”等级。通过在受害者受骗访问的网站上托管恶意内容或诱使受害者打开经特殊设计的恶意文件，攻击者可以利用这些严重漏洞完全控制系统。对于被列为“重要”等级的漏洞，攻击者利用漏洞的方式相同，但导致的结果是向攻击者泄露内存中的内容。

MS17-012 公告修复了 5 个重要漏洞和一个严重漏洞。严重漏洞与无法正确验证客户端输入的 Internet 存储名称服务 (iSNS) 服务器服务相关。攻击者有可能利用此漏洞，在受影响的系统上使用 SYSTEM 帐户运行任意代码。重要漏洞包括 Device Guard 中允许攻击者修改 PowerShell 脚本而不会使文件签名无效的漏洞；SMBv2 和 SMBv3 中的拒绝服务漏洞；以及加载某些 DLL 文件时的远程代码执行漏洞。

包括 Microsoft Office 和 Silverlight 在内，许多不同程序都使用 Microsoft Windows 图形组件。MS17-013 描述了该组件中的 2 个严重漏洞和 10 个重要漏洞。通过诱使受害者访问托管恶意内容的网站或让受害者打开恶意文件，攻击者可以利用这两个严重漏洞远程执行代码。重要漏洞与 Windows Graphic 设备接口处理内存中对象的方式相关，导致的结果包括允许本地用户在内核模式下执行代码、远程用户发现内存内容，或帮助绕过地址空间布局随机化 (ASLR) 防护功能。

星期二补丁从来都不会缺少 Adobe Flash Player 公告，此次发布的 MS17-023 也修复了 Adobe 安全公告 APSB17-07 中另有描述的严重漏洞。此更新修复了 Adobe Flash Player 中的一系列远程代码执行漏洞。如果无法修复或删除 Adobe Flash Player，该公告还介绍了许多防止 Flash Player 执行的解决办法。

列为重要等级的公告

MS17-014、MS17-015、MS17-016、MS17-017、MS17-018、MS17-019、MS17-020、MS17-021 和 MS17-022 被列为“重要”等级。

尽管 MS17-014 修复了 Microsoft Office 中的 12 个漏洞，但这些漏洞中没有一个被列为“严重”等级（不过它们全都是重要漏洞）。攻击者可以利用其中的 7 个漏洞，借用户之手打开恶意文档或访问托管恶意内容的网站，以与本地用户相同的权限执行任意代码。另外几个漏洞则允许攻击者对 Microsoft Office 执行拒绝服务攻击、泄露内存内容、方便实施跨站点脚本

(XSS) 攻击，以及通过错误验证的证书篡改受信任的通信。

MS17-015 和 MS17-016 分别描述了 Microsoft Exchange Outlook Web Access 和 Microsoft IIS Server 中被列为“重要”等级的一个漏洞。攻击者可以利用 Outlook Web Access 漏洞，在受害者点击邮件或聊天客户端中的恶意链接后执行内容注入攻击。而利用 IIS Server 漏洞，攻击者可以执行跨站点脚本攻击 (XSS) 并以与当前用户相同的权限运行脚本；同样，受害者必须点击恶意链接，攻击才能成功。

MS17-017 和 MS17-018 修复了 Windows 内核和 Windows 内核模式驱动程序中的 12 个重要漏洞。利用这些漏洞，通过本地身份验证的用户或具有本地访问权限的用户就可以不当升级权限。

公告 MS17-019、MS17-020、MS17-021、MS17-022 分别与 Active Directory 联合身份验证服务、Windows DVD Maker、DirectShow 和 XML Core Services 中的一个重要漏洞相关。攻击者可以利用这一系列漏洞从受影响的系统收集信息。在 Windows DVD Maker 中，攻击者必须通过本地身份验证才能触发攻击。后两个漏洞需要受害者访问恶意网站后，攻击者才能利用漏洞进行攻击。

防护

为了响应此次 Microsoft 公告，Talos 发布以下规则来修复这些漏洞。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 SID：41549-41556、41561-41598、41601-41602、41605-41610、41633-41634、41763-41764、41926-41961、41964-41998

发布者：MARTIN LEE 发布时间：17:26
标签：CVE、MICROSOFT、星期二补丁、漏洞