2016 年 10 月 11 日，星期二

Microsoft 星期二补丁 - 2016 年 10 月

又到了星期二补丁的发布时间！为修复漏洞，Microsoft 每月发布安全公告。本月的公告为 37 个新披露的安全漏洞提供了修复程序。Microsoft 在本日的星期二补丁中共发布了 10 个公告，其中有 5 个公告被评为“严重”等级，分别修复了 Edge、图形组件、Internet Explorer、Video Control 和 Adobe Flash Player 中的漏洞。4 个公告被评为“重要”等级，分别修复了 Office、Windows 诊断中心、Windows 内核模式驱动程序和 Windows 注册表中的漏洞。1 个公告被评为“中等”等级，修复了 Microsoft Internet 消息发送 API 中的一个漏洞。

列为严重等级的公告

列为“严重”等级的公告如下：MS16-118、MS16-119、MS16-120、MS16-122、MS16-127

MS16-118 和 MS16-119 分别是本月修复 Internet Explorer 和 Edge 漏洞的公告。Internet Explorer 公告修复了 11 个漏洞，Edge 公告修复了 13 个漏洞。有 7 个漏洞同时影响 Edge 和 IE。所修复的大部分漏洞属于会导致任意代码执行的内存损坏漏洞，本月发布的公告中还修复了一些权限提升和信息泄露漏洞。

MS16-120 修复了 Microsoft 图形组件中的 7 个漏洞。其中 CVE-2016-3393 和 CVE-2016-3396 这两个漏洞分别是 GDI 组件和字体库中的任意代码执行漏洞。如果用户访问由攻击者为利用这些漏洞而精心设计的网站或打开这样的文件，就可能成为这些漏洞的受害者。两个权限提升漏洞 CVE-2016-3270 和 CVE-2016-7182 也得到了修复。利用这两个漏洞，通过解析 TrueType 字体或精心设计的应用可以将用户权限提升为管理员权限。剩余三个漏洞（CVE-2016-3209、CVE-2016-3262 和 CVE-2016-3263）是可被利用来逃避 ASLR 的信息泄露漏洞。

MS16-122 修复了 Microsoft Video Control 中的任意代码执行漏洞 CVE-2016-0142。此漏洞表现为无法正确处理内存中的对象。如果用户打开攻击者精心设计的文件或启动恶意可执行程序，此漏洞就可能会被利用。发动这种攻击的场景包括邮件攻击，或用户下载文件/可执行文件并在自己的计算机上打开。

MS16-127 更新了在 Internet Explorer 和 Edge 中嵌入的 Adobe Flash Player 并处理了已在 APSB16-32 中修复的所有漏洞。有关此 Adobe Flash Player 公告的更多详情，请参见 Adobe 网站上发布的公告。

列为重要等级的公告

列为“重要”等级的公告如下：MS16-121、MS16-123、MS16-124、MS16-125

MS16-121 在支持的所有 Microsoft Office 版本中修复了任意代码执行漏洞 CVE-2016-7193。CVE-2016-7193 表现为在 Office 解析和处理丰富文本格式 (RTF) 文件时出现的内存损坏漏洞。此漏洞要发挥作用，必须要诱骗用户打开攻击者专为利用此漏洞而设计的文件。

MS16-123 修复了在 Windows 内核模式驱动程序中发现的 5 个本地权限提升漏洞。这 5 个漏洞全都可能被利用。已验证的用户执行攻击者为利用其中某个漏洞而精心设计的二进制文件时，会将用户权限提升为管理员权限。其中 4 个漏洞（CVE-2016-3266、CVE-2016-3376、CVE-2016-7185 和 CVE-2016-7211）在内核自身中出现，第 5 个漏洞 (CVE-216-3341) 在 Windows 事务管理器中出现。

MS16-124 修复了 Windows 内核中的四个本地权限提升漏洞。这 4 个漏洞（CVE-2016-0070、CVE-2016-0073、CVE-2016-0075 和 CVE-2016-0079）均表现为 Windows 内核 API 错误地允许用户检索注册表信息，而这些信息可被用于将用户权限提升为管理员权限。当目标计算机启动由攻击者精心设计的可执行文件时，这些漏洞就可能被利用。

MS16-125 修复了 Windows 诊断中心中的一个权限提升漏洞 CVE-2016-7188。CVE-2016-7188 在 Windows 诊断中心标准收集器服务未能正确审查用户输入，从而导致不安全的库加载时出现。此漏洞要发挥作用，必须要诱骗已验证的用户打开攻击者专为利用此漏洞而设计的可执行文件。

列为中等等级的公告

MS16-126 是本月唯一一个被列为“中等”等级的安全公告，修复了 Microsoft Internet 消息发送 API 中的一个重要消息泄露漏洞 CVE-2016-3298。CVE-2016-3298 是与处理内存中对象相关的一个漏洞，成功利用此漏洞的攻击者可以测试磁盘上是否存在文件。如果用户访问利用该漏洞的恶意网站，就可能成为此漏洞的受害者。

防护

为了响应上述公告，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，请参阅防御中心或 Snort.org。

Snort 规则

Microsoft 公告：40364-40381、40383-40405、40408-40412、40418-40428

发布者：Alexander Chiu；发布时间：16:57
标签：Adobe Flash、Edge、Internet Explorer、Microsoft、Office、星期二补丁、Snort 规则