2016 年 4 月 12 日，星期二

MICROSOFT 星期二补丁 - 2016 年 4 月

Microsoft 4 月的星期二补丁已经发布，其中包括帮助解决 Microsoft 产品安全漏洞的最新月度安全公告集。本月发布的 13 个公告涉及到 31 个漏洞。其中有 6 个公告解决了在 Edge、图形组件、Internet Explorer、XML 核心服务、Microsoft Office 和 Adobe Flash Player 中被评为“严重”等级的漏洞。其余 7 个公告解决了 Hyper-V、Microsoft Office 和其他 Windows 组件中的重要漏洞。

评为严重等级的公告

在本月的发布中，公告 MS16-037 至 MS16-040 以及公告 MS16-042 和 MS16-050 被列为严重等级。

MS16-037 与 Internet Explorer 中的六个漏洞相关。其中最严重的漏洞会导致用户在浏览攻击者特别设计的网站时，攻击者可以利用浏览器中的内存损坏漏洞在用户设备上执行任意代码。虽然攻击者只能使用与当前用户相同的管理权限来执行代码，但是对于很多具有完整管理员权限的用户来说，攻击者可以利用此漏洞完全控制设备。要利用此漏洞，攻击者必须诱使受害者查看攻击者控制的内容。过去，这一点并未对攻击者构成主要限制。因为，攻击者擅长通过发送垃圾邮件、侵害合法网站，以及滥用网络广告网络等手段，将用户重定向到恶意网站。

MS16-038 解决了 Microsoft Edge 浏览器中的五个其他远程代码执行漏洞，以及 IE 和 Edge 共有的一个漏洞，该漏洞在 MS16-037 中也有介绍。这些漏洞中最严重的漏洞还会导致攻击者能够利用内存损坏漏洞而在受害者的设备上执行任意代码。如前所述，攻击者可以制作一个恶意网站来利用这些漏洞侵害受害者的设备。

MS16-039 解决了 Windows 内核模式驱动程序中的三个重要权限升级漏洞，以及 Windows 字体库中允许执行远程代码的严重漏洞 CVE-2016-0145。Microsoft 以前就曾发现并修补嵌入字体中的漏洞，尤其是 2015 年 7 月的带外更新 MS15-078 中发现的远程代码漏洞，以及 2013 年 7 月的 MS13-053 和 MS13-054 中解决的字体漏洞。对攻击者而言，嵌入字体中的漏洞是特别有用的攻击媒介，因为它们可以包含在恶意网站和 Microsoft Office 文档中。

进一步的远程代码执行漏洞已通过 MS16-040 和 MS16-042 解决。MS16-040 解决了 XML 核心服务容易受到专门设计用于执行任意代码的 XML 代码攻击的情况；MS16-042 则解决了导致 Microsoft Office 易受攻击的四个单独远程代码执行漏洞。这些漏洞中唯一被评为“严重”等级（而非“重要”等级）的是 CVE-2016-0127，此漏洞可以将预览窗格作为攻击媒介。

MS16-050 是 Microsoft 对 Adobe 安全公告 APSB16-10 做出的回应，它解决了 Windows 8.1、Windows Server 2012 和 Windows 10 等多个平台中的十个不同的 Adobe Flash Player 漏洞。这些漏洞中的一个当前正在被 Magnitude 漏洞攻击包利用。该公告包含通过修改注册表以及应用组策略来禁用 Flash Player 的有用说明。管理员可能需要仔细考虑按照这些方法在他们所负责的设备中删除 Flash Player 的利弊。

评为重要等级的公告

Microsoft 公告 MS16-041 以及 MS16-044 至 MS16-049 被评为重要等级。

MS16-041 解决了 Microsoft .NET Framework 中的漏洞 CVE-2016-0148。在某些 Microsoft 操作系统上，此漏洞可用于执行远程代码，但仅限于攻击者已经具有本地系统访问权限的情况下。在某些环境中，该漏洞可用于执行拒绝服务攻击，而其他 Microsoft 操作系统则不会受此漏洞影响。

MS16-044 解决了 CVE-2016-0153，Microsoft OLE 内的一个远程代码执行漏洞。Windows 10 不受此漏洞影响。

MS16-045 解决了 Hyper-V 中的三个漏洞。其中，CVE-2016-0088 允许访客操作系统上的用户在 Hyper-V 主机上执行任意代码。另外两个漏洞允许访客操作系统上的用户从 Hyper-V 操作系统读取内存信息。

MS16-046 解决了 Windows 10 中允许经过身份验证的用户升级权限，并以管理员身份执行任意代码的漏洞。MS16-048 解决了客户端/服务器运行时子系统无法正确管理内存中的进程令牌时权限进一步升级的漏洞，该漏洞允许经过身份验证的用户绕过安全功能并以管理员身份执行代码。

MS16-047 解决的是一个潜在漏洞，攻击者可以通过发动中间人攻击使 RPC 通道身份验证降级，从而冒充经过身份验证的用户。通过在安全帐户管理器和本地安全机构域策略远程协议中利用此漏洞，攻击者就能访问安全帐户管理器数据库。

MS16-049 解决了 Windows 10 HTTP 2.0 协议堆栈 (HTTP.sys) 中的拒绝服务攻击漏洞。攻击者可以通过创建特别设计的 HTTP 2.0 请求，使存在漏洞的系统失去响应能力。

覆盖范围

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，请参阅防御中心、FireSIGHT 管理中心或 Snort.org。

SNORT 规则

- Microsoft 相关规则：38458 - 38464、38469 - 38470、38473 - 38474、38479 - 38484、38489 - 38490、38495 - 38496、38503 - 38506
- 相关 Adobe 公告：38401 - 38402、38413 - 38416、38425 - 38428

发布者：ALEXANDER CHIU；发布时间：下午 4:12
标签：ADOBE FLASH、INTERNET EXPLORER、MICROSOFT、OFFICE、星期二补丁、WINDOWS