2016 年 9 月 13 日，星期二

Microsoft 星期二补丁 - 2016 年 9 月

作者：Jaeson Schultz。

又到了 Microsoft 星期二补丁的发布时间，这意味着我们必须准备好武装我们的系统，使之免受新一轮安全漏洞的影响。Microsoft 本月已发布涵盖五十 (50) 种安全漏洞的十四 (14) 个公告。其中七个公告的严重性被视为“严重”等级。这些“严重”等级的公告影响 Internet Explorer、Microsoft Edge、Microsoft 图形组件、Microsoft Exchange Server、Microsoft Office、适用于 VBScript Scripting Engine 的 OLE Automation 和 Adobe Flash Player。其余七个公告影响的产品包括 Silverlight、Windows、Windows Kernel、Windows Lock Screen、Windows Secure Kernel Mode、Windows SMBv1 Server 和 Microsoft Windows PDF Library 等。

评为严重等级的公告

在本月的发布中，公告 MS16-104、MS-105、MS16-106、MS16-107、MS16-108、MS16-116 和 MS16-117 被列为“重要”等级。

MS16-104 和 MS-105 分别是本月关于 Internet Explorer 和 Microsoft Edge 的安全公告。这些公告共解决二十二 (22) 种漏洞，主要包括内存破坏和信息泄露漏洞。六 (6) 种漏洞是共有漏洞，同时影响 IE 和 Edge。影响这两种产品的最严重漏洞为内存破坏漏洞 CVE-2016-3295，涉及存储器中的对象处理方式。通过将用户定向至特制网页，攻击者可实现远程代码执行。

MS16-106 解决 Microsoft 图形组件中的少量漏洞。最严重漏洞 CVE-2016-3356 影响 Windows 图形设备接口 (GDI) 处理存储器中对象的方式。攻击者可通过将受害者定向至特制网页或诱使受害者打开特制网页文档文件实现远程代码执行。

MS16-107 修复 Microsoft Office 中的十三种漏洞。大部分漏洞为内存破坏漏洞，再加上安全功能绕行和电子欺骗漏洞。这一组中的最严重漏洞为 CVE-2016-3357。如果攻击者可以说服受害者打开特制 MS Office 文件，则可能实现远程代码执行。

MS16-108 解决 Microsoft Exchange 中的三种漏洞。Talos 博客的忠实读者可能还记得，在 7 月我们讨论了 Talos 在 Oracle Outside In Technology 中发现的几大漏洞。Oracle Outside-In 是用于帮助解析多种文件类型的软件库。通过创建自定义文件，攻击者可能实现远程代码执行。

MS16-116 解决适用于 VBScript Scripting Engine 的 Window OLE Automation 中的脚本漏洞。要在受害者计算机上利用此漏洞和执行代码，攻击者可能必须说服受害者访问已遭到危害的网站或恶意网站。请注意，据 Microsoft 称，必须安装两次更新，才能免受漏洞影响，即必须安装本更新和公告 MS16-104 中所包含的更新。

MS16-117 更新了 Internet Explorer 和 Microsoft Edge 中所包含的 Adobe Flash 库。该公告修复了 Adobe 安全公告 APSB16-29 所确定的二十九 (29) 种漏洞。老实说，Adobe Flash 中所确定的漏洞源源不断，用户最好采取措施阻止 Flash 在无人监管的 Web 浏览器中运行。

评为重要等级的公告

MS16-109 解决 Microsoft Silverlight 如何在 StringBuilder 中将内存分配用于插入和追加字符串方面存在的单个漏洞。通过诱导受害者查看自定义 silverlight 应用，可实现远程代码执行。

MS16-110 解决 Microsoft Windows 中的四种漏洞。通过利用此公告所解决的漏洞，攻击者可能会升级权限、暴力破解用户的 NTLM 密码散列、执行拒绝服务攻击，甚至利用提升的特权执行任意代码。

MS16-111 修复 Windows Kernel 中的少量权限升级漏洞。这些漏洞均为权限升级漏洞，攻击者可通过在系统上执行自定义设计应用触发这些漏洞。

MS16-112 解决 Windows Lock Screen 中的一个漏洞。在有些情况下，用户的 Windows 锁屏可能会加载网页内容。如果攻击者可通过物理方式访问受害者锁定的计算机，则可以将该计算机连接到恶意 WiFi 热点，或将移动宽带适配器插入受害者计算机。利用此漏洞后，攻击者可以在受害者计算机上运行代码。

MS16-113 解决有关 Windows Secure Kernel Mode 如何处理存储器中的对象的一个信息泄露漏洞。通过本地身份验证的攻击者可通过在目标系统上运行应用利用此漏洞。请注意，单独的这个信息泄露漏洞并不足以危害系统。攻击者必须利用此漏洞加上其他漏洞才能攻击系统。

MS16-114 解决 Windows Server Message Block 1.0 (SMBv1) Server 中的单个远程代码执行漏洞。要利用此漏洞，攻击者首先需进行 SMBv1 服务器身份验证，并能够打开受害者 SMBv1 服务器上的文件。

MS16-115 修复 Microsoft Windows PDF 库中的一对信息泄露漏洞。这对漏洞涉及 Windows PDF 库如何处理存储器中的对象。成功利用这些漏洞后，攻击者可获取更多信息，然后将这些信息用于进一步攻击目标系统。

防护产品

Talos 已发布如下 Snort 规则，以响应 Microsoft 和 Adobe 披露的这些公告信息。请注意，这些规则会根据新的漏洞信息而有所变更。如需获取最新信息，请参阅 FireSIGHT 防御中心或 Snort.org。

- Microsoft 公告 SID：40129、40146、40035-40036、40073-40080、40082-40124、40127-40128、40132-40145、40147-40150
- Adobe 公告 SID：40151-40181

发布者：JAESON SCHULTZ；发布时间：20:01

标签：ADOBE、MICROSOFT、补丁、星期二补丁、SNORT 规则、漏洞