2016 年 8 月 9 日，星期二

Microsoft 星期二补丁 - 2016 年 8 月

作者：Edmund Brumaghin 和 Jonah Samost

Microsoft 发布了 2016 年 8 月的星期二补丁，其中包括修复一系列 Microsoft 产品安全漏洞的若干安全公告和相关补丁。本月发布的补丁包括 9 个公告，共修复了 28 个漏洞。其中有 5 个公告被列为“严重”等级，分别修复了 Internet Explorer、Edge、Windows 图形组件、Microsoft Office 和 Windows PDF 库中的漏洞。其余公告均为“重要”等级，分别修复了 Windows 内核模式驱动程序、安全启动、Windows 身份验证方法和 ActiveSyncProvider 中存在的漏洞。

列为严重等级的公告

在本月的发布中，Microsoft 将公告 MS16-095、MS16-096、MS16-097、MS16-099 和 MS16-102 列为“严重”等级。

MS16-095 和 MS16-096 是本月关于 Microsoft Internet Explorer 和 Edge 安全漏洞的公告。Internet Explorer 公告共解决了 9 个漏洞，包括 5 个内存损坏漏洞和 4 个信息泄漏漏洞。Edge 公告共涉及 8 个漏洞，包括 1 个远程代码执行漏洞、4 个内存损坏漏洞和 3 个信息泄漏漏洞。Internet Explorer 公告对 Windows 客户端的影响被列为“严重”等级，对 Windows 服务器的影响被列为“中等”等级。

MS16-097 解决了 Windows 图形组件中存在的 3 个远程代码执行漏洞（CVE-2016-3301、CVE-2016-3303 和 CVE-2016-3304）。这些漏洞与 Windows 图形组件处理字体的方式相关，攻击者可以利用这些漏洞在受影响的系统上获得代码执行权限。这些漏洞可影响所有受支持的 Microsoft Windows 版本，而且会影响 Microsoft Office、Microsoft Lync 和 Skype for Business 的多个版本。

MS16-099 解决了各种版本的 Microsoft Office 中存在的 4 个漏洞，包括 1 个信息泄漏漏洞和 3 个内存损坏漏洞。利用内存损坏漏洞，攻击者可以在用户打开经特殊设计的 Office 文档后，获得与当前用户相同的权限，从而远程执行任意代码。此更新解决了漏洞 CVE-2016-3313、CVE-2016-3316、CVE-2016-3317 和 CVE-2016-3318。

MS16-102 修复了 Microsoft Windows PDF 库中存在的一个漏洞：CVE-2016-3319。此漏洞可用于制作经特殊设计的 PDF 文档，如果在受影响的系统中打开该文档，攻击者将能够以与当前用户相同的权限执行代码。在将 Microsoft Edge 配置为默认浏览器的 Windows 10 系统中，只要浏览托管恶意 PDF 的网站，就会触发此漏洞，因为 Edge 会尝试自动渲染文件内容。对于所有受支持的 Windows 8.1、Windows Server 2012、Windows Server 2012 R2 和 Windows 10 版本，此漏洞均被列为“严重”等级。

列为重要等级的公告

在本月的发布中，Microsoft 将公告 MS16-098、MS16-100、MS16-101 和 MS16-103 列为“重要”等级。

MS16-098 解决了多个本地权限提升漏洞，这些漏洞可在从 Windows Vista 到 Windows Server 2012 R2 等多种系统中触发。如果特定 Windows 内核模式驱动程序无法正确处理内存中的对象，则会造成这些漏洞。通过利用这些漏洞，攻击者可以在内核模式下运行任意代码。Microsoft 为这些漏洞分配了 4 个 CVE 编号（CVE-2016-3308 至 CVE-2016-3311）。

MS16-100 修复了一个安全引导绕过漏洞。如果攻击者拥有目标设备的物理访问权限或管理权限，便可以利用该漏洞。当 Windows 安全启动错误地加载引导管理器时，便会触发该漏洞。成功利用此漏洞的攻击者可以绕过 BitLocker 的安全启动完整性验证，禁用代码完整性检查，允许加载经测试签名的驱动程序或可执行文件，或者执行其他恶意活动。该漏洞可以影响从 Windows 8.1 到 Windows 10 等各种系统所有受支持的版本，漏洞编号为 CVE-2016-3320。

MS16-101 解决了两个权限提升漏洞。CVE-2016-3300 是 Windows Netlogon 与运行 Windows Server 2012 或 Windows Server 2012 R2 的域控制器的系统建立安全连接的方式中存在的漏洞。要利用此漏洞并提升对已加入域的计算机的权限，攻击者需要获取已加入域并指向上述系统之一的计算机的访问权限。CVE-2016-3237 产生的原因是 Kerberos 不正确地处理密码更改请求，并回退到作为默认身份验证协议的 NTLM 身份验证协议。要利用此漏洞并绕过 Kerberos 身份验证机制，攻击者需要对目标计算机与其域控制器之间的流量发动中间人攻击。Kerberos 权限提升漏洞可影响所有受支持的 Windows 版本；Netlogon 漏洞仅影响所有受支持的 Windows 8.1 和 Server 2012 版本。

MS16-103 修复了 Universal Outlook 服务在未能建立安全连接时存在的一个信息泄漏漏洞。攻击者可以利用该漏洞获取用户的用户名和密码。该漏洞可影响所有受支持的 Windows 10 版本，漏洞编号为 CVE-2016-3312。

覆盖

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、FireSIGHT 管理中心或 Snort.org。

Snort 规则：

39808-39829、39831-39844
发布者：Edmund Brumaghin；发布时间 15:15
标签：Microsoft、Office、星期二补丁、Snort 规则、Windows