2016 年 6 月 14 日，星期二

MICROSOFT 星期二补丁 - 2016 年 6 月

作者：Warren Mercer。

Microsoft 2016 年 6 月的星期二补丁已经发布，其中包括修复 Microsoft 产品安全漏洞的一系列月度安全公告集。本月发布的 16 个公告修复了 44 个漏洞。五个公告解决在 MS DNS 服务器、Edge、Internet Explorer、JScript/VBScript 和 Office 中发现的严重漏洞。其余公告均为“重要”等级，分别修复了 Active Directory、Exchange Server、组策略、SMB 服务器、Netlogon、Windows Graphic 组件、Windows 内核模式驱动程序、Windows PDF、Windows Search 组件和 WPAD 中的漏洞。

评为严重等级的公告

在本次发布中，Microsoft 公告 MS16-063 和 MS16-068 至 MS16-071 被列为“严重”等级。

MS16-063 和 MS16-068 是本月关于 Microsoft Internet Explorer 和 Edge 浏览器的公告。IE 安全公告修复了 Internet Explorer 版本 9、10 和 11 中的漏洞。IE 公告总共涵盖十个漏洞，其中包括八个内存损坏漏洞（其中七个是严重漏洞）、一个 XSS 过滤器漏洞和一个 WPAD 漏洞。Edge 公告修复了八个漏洞，包括四个内存损坏漏洞、两个信息泄露漏洞、一个安全功能绕过漏洞和一个 PDF 远程代码执行漏洞。

MS16-069 修复了 Windows 中的 JScript 和 VBScript 脚本引擎内的六个任意代码执行漏洞。需要注意的是，该公告面向 Windows Vista、Windows Server 2008 和 Windows Server 2008 R2。使用较新版本 Windows 的用户不会看到此公告。引擎处理 IE 内存中对象的方式导致了多个任意代码执行漏洞。这些漏洞可能被用于漏洞攻击，例如，网络攻击者可以创建恶意网站，利用这些漏洞以当前用户身份运行代码。另一种攻击方式是利用嵌入恶意 ActiveX 控件的 Microsoft Office 文档。对于无法应用此安全更新的用户，Microsoft 建议了一种解决办法。有关更多信息，请参阅 Microsoft 安全公告。

MS16-070 修复了 Microsoft Office 中的四个漏洞。本月的公告中修复了三个任意代码执行漏洞和一个信息泄露漏洞。在三个代码执行漏洞中，有两个是由于内存损坏 (CVE-2016-0025, CVE-2016-3233) 而造成，一个是由于 OLE DLL 端加载 (CVE-2016-3235) 而造成。攻击者可以利用经特殊设计的电子邮件诱使用户打开附件，从而成功利用这些漏洞。此漏洞会导致网络攻击者以登录用户身份获得任意代码执行权限。

MS16-071 修复了 Microsoft DNS 服务器中的释放后使用漏洞 (CVE-2016-3227)。成功利用此缺陷的网络攻击者可以创建一个经特殊设计的应用，以连接到 Windows DNS 服务器并向服务器发出恶意请求，从而使用本地 SYSTEM 帐户执行任意代码。

评为重要等级的公告

在本月的发布中，Microsoft 公告 MS16-072 至 MS16-082 被列为“重要”等级。

MS16-072 修复了 CVE-2016-3223，组策略中的一个权限提升漏洞。此漏洞在 Windows 处理组策略更新时出现。请注意，要利用此漏洞发动攻击，攻击者需要在域控制器和目标机器之间发动中间人攻击 (MiTM)。这样，用户帐户就会升级为享有特权的管理帐户。

MS16-073 修复了 CVE-2016-3218 和 CVE-2016-3221，Win32k 内核驱动程序中的权限提升漏洞。利用这些缺陷，攻击者可以在内核模式下执行任意代码。当 Windows 内核模式驱动程序无法正确处理内存中的对象时，这些漏洞便有机会被利用。此通告还修复了信息泄露漏洞 (CVE-2016-3232)，但仅特定于 Windows Server 2012 版本。当 Windows Virtual PCI 和虚拟服务提供程序无法正确处理未初始化的内存时，便存在此漏洞。成功利用此漏洞的攻击者可能会泄露内存中的特定信息。

MS16-074 修复了 Microsoft Graphic 组件中的两个权限提升漏洞和一个信息泄露漏洞。CVE-2016-3216 是 Windows Graphic 设备接口 (GDI32.dll) 中的信息泄露漏洞，由于未正确处理内存中的对象而引起。此漏洞会导致绕过 ASLR，如果与另一漏洞配合使用，可以实现任意代码执行。两个权限提升漏洞都与无法正确处理内存相关，CVE-2016-3219 会影响 Windows Graphic 组件，CVE-2016-3220 会影响 Adobe Type Manager 字体驱动程序 (ATMFD)。成功利用这些漏洞的攻击者可能会作为管理员执行任意命令。

MS16-075 修复了 CVE-2016-3225，Microsoft 服务器消息块协议中的任意代码执行缺陷。利用此漏洞，经验证的攻击者可以将身份验证请求转发给另一项服务，并使用提升的权限执行任意代码。根据 Microsoft 的详细说明，要利用此攻击，攻击者必须已登录到受影响的计算机。

MS16-076 修复了 CVE-2016-3228，NetLogon 中由于无法正确处理对象而导致的内存损坏远程代码执行漏洞。利用此漏洞，攻击者可以访问组织的主域控制器 (PDC)，运行经特殊设计的应用来执行远程代码，并与作为副本域控制器的 PDC 建立安全通道。

MS16-077 修复了两个与 Windows 代理自动发现 (WPAD) 相关的漏洞，这两个漏洞均允许权限提升。此更新解决了 Windows 处理代理发现的方式。当 Windows 回退到易受攻击的代理发现进程时，即存在 CVE-2016-3213。要利用此漏洞，攻击者需要让受害者的 DNS 服务器感染病毒，以便将他们的主机注册为本地 DNS 中的 WPAD 或响应 WPAD 的 NetBIOS 名

称请求。在处理某些代理发现方案时，Windows 存在允许权限提升的漏洞 CVE-2016-3236。此漏洞可能会让攻击者能够访问和控制网络流量。

MS16-078 修复了 CVE-2016-3231，Windows Diagnostic Hub 中的权限提升缺陷。当标准收集器服务无法正确清理输入时，攻击者可以利用此漏洞获得特权提升，从而导致不安全的库加载行为。成功利用此漏洞的攻击者可以使用提升的系统特权运行任意代码。

MS016-079 修复了 Microsoft Exchange Server 中的漏洞 (CVE-2016-0028)：当 Outlook Web Access (OWA) 无法正确处理 HTML 消息时，可能导致信息泄露。如果攻击者在 OWA 邮件中发送从攻击者控制的 URL 加载的（在未警告或筛选的情况下）经特殊设计的图像 URL，便有可能回传最终用户的信息，采集用户的指纹，并跟踪用户。

MS16-080 修复了 Microsoft PDF 中的多个漏洞。CVE-2016-3201 与 CVE-2016-3215 均为信息泄露漏洞，可能导致攻击者使用经特殊设计的 PDF 文件成功读取用户环境中的信息。CVE-2016-3203 是一个远程代码执行缺陷，攻击者可通过诱使用户打开恶意 PDF 文件来利用此漏洞。此公告旨在通过更正 .pdf 文件在 Windows 中的解析方式来修复这些问题。

MS16-081 修复了 Microsoft Active Directory 内的拒绝服务 (DoS) 漏洞。利用此漏洞，攻击者可通过创建多个计算机帐户导致 AD 无响应。此漏洞可用来在 AD 环境中使用已经过身份验证的帐户创建多个计算机帐户。CVE-2016-3226 已通过更正在 AD 中创建计算机帐户的方式得到修复。

MS16-082 修复了 CVE-2016-3230，Microsoft Windows StructuredQuery 组件中的拒绝服务 (DoS) 漏洞。当 StructuredQuery 组件无法正确处理内存中的对象时，便会出现此漏洞。攻击者可利用此漏洞使服务器的性能显著下降，从而产生 DoS 条件。

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，请参阅防御中心或 Snort.org。

Snort 规则：

- Microsoft 公告：39227、39193-39196、39199-39208、39211-39226、39228-39239、39242-39261、39266-39267

发布者：ALEXANDER CHIU；发布时间：16:26

标签：MICROSOFT、OFFICE、星期二补丁、SNORT 规则、WINDOWS