2016 年 12 月 13 日，星期二

Microsoft 星期二补丁 - 2016 年 12 月

2016 年的最后一个星期二补丁已发布。今天，Microsoft 发布了修复其产品中的安全漏洞的月度安全公告集。本月发布的 12 个公告修复了 48 个漏洞。其中有 6 个公告被列为“严重”等级，分别修复了 Internet Explorer、Edge、Microsoft 图形组件、Microsoft Uniscribe 和 WAdobe Flash Player 中的漏洞。其余 7 个公告均为“重要”等级，分别修复了内核、加密驱动程序及安装程序等各种 Windows 组件中存在的漏洞。

列为严重等级的公告

在本次 Microsoft 发布中，公告 MS16-144 至 MS16-148 以及公告 MS16-154 被列为“严重”等级。

MS16-144 是本月关于 Internet Explorer 的公告。共修复了 9 个漏洞，包括各种内存损坏漏洞（CVE-2016-7202、CVE-2016-7279、CVE-2016-7283、CVE-2016-7287、CVE-2016-7293）、安全功能绕过漏洞（CVE-2016-7281、CVE-2016-7282），以及信息泄露漏洞（CVE-2016-7278、CVE-2016-7284）。如果用户使用 Internet Explorer 查看经特殊设计的网页，那么其中最严重的漏洞可能导致远程代码执行。这些漏洞影响 Internet Explorer 版本 9、10 和 11。漏洞的严重性与使用的 Internet Explorer 和 Windows 版本相关。Windows Vista 7、8.1 和 10 都受到影响。此外，Windows Server 2008、2012 和 2016 也受到影响。请注意，Windows 服务器漏洞被列为“中等”等级，而客户端版本都被列为“严重”等级。

MS16-145 是本月关于 Edge 浏览器的公告。共修复了 11 个漏洞，包括各种内存损坏漏洞（CVE-2016-7181、CVE-2016-7279、CVE-2016-7286、CVE-2016-7287、CVE-2016-7288、CVE-2016-7296、CVE-2016-7297）、安全功能绕过漏洞（CVE-2016-7281、CVE-2016-7282），以及信息泄露漏洞（CVE-2016-7206、CVE-2016-7280）。如果用户使用 Internet Explorer 查看经特殊设计的网页，那么其中最严重的漏洞可能导致远程代码执行。这些漏洞仅影响 Windows 10 和 Windows Server 2016。Windows 10 漏洞均被列为“严重”等级，Windows Server 2016 漏洞列为“中等”等级。

MS16-146 公告修复了 Windows 图形组件中的 3 个漏洞。如果用户访问经特殊设计的网站或打开经特殊设计的文档，则其中最严重的漏洞可能导致远程代码执行。修复的漏洞包括两个内存损坏漏洞（CVE-2016-7272、CVE-2016-7273）和一个信息泄露漏洞 (CVE-2016-7257)。这些漏洞影响 Windows Vista 7、8.1、10、Server 2008、Server 2008 R2、Server 2012、Server 2012 R2 和 Server 2016。

MS16-147 修复了 Windows Uniscribe 中的一个远程代码执行漏洞 (CVE-2016-7274)。如果访问经特殊设计的网站或打开经特殊设计的文档，则会触发此漏洞。Windows Uniscribe 处理内存中的对象的方式可导致此漏洞。此漏洞影响所有当前受支持的 Windows 版本。

MS16-148 是本月关于 Microsoft Office 的公告。共修复了 16 个漏洞，包括各种内存损坏漏洞（CVE-2016-7263、CVE-2016-7277、CVE-2016-7289、CVE-2016-7298）、信息泄露漏洞（CVE-2016-7257、CVE-2016-7264、CVE-2016-7265、CVE-2016-7268、CVE-2016-7276、CVE-2016-7290、CVE-2016-7291）、安全功能绕过漏洞（CVE-2016-7262、CVE-2016-7266、CVE-2016-7267）、权限提升漏洞 (CVE-2016-7300)，以及单个 OLE DLL 端加载漏洞 (CVE-2016-7275)。如果用户打开经特殊设计的 Office 文档，则其中最严重的漏洞可能导致远程代码执行。Windows 和 Mac 版本的 Office 都会受到影响。这包括 Office 2007、2010、2013、2016 以及 Office 2011 for Mac 2011 和 2016。此外，Microsoft Sharepoint Server 2007 和 2010 以及 Office Web Apps 2010 上的 Office 服务也会受到影响。

MS16-154 是本月关于 Adobe Flash Player 的公告。共修复了 15 个可能导致远程代码执行的漏洞。如果用户访问经特殊设计的网站，那么其中最严重的漏洞可能导致远程代码执行。这会影响运行 Adobe Flash Player 的 Windows 的所有受支持版本。唯一替代缓解措施是阻止在 Internet Explorer 和 Microsoft Office 中运行 Flash Player。这可以在本地或通过组策略来实现。

列为重要等级的公告

Microsoft 公告 MS16-149 至 MS16-153 以及公告 MS16-155 列为“重要”等级。

MS16-149 修复了 2 个漏洞，一个是 Windows Crypto 驱动程序中的信息泄露漏洞 (CVE-2016-7219)，另一个是 Windows Installer 中的权限提升漏洞 (CVE-2016-7292)。如果本地攻击者运行经特殊设计的应用，则其中最严重的漏洞可能导致权限提升。这些漏洞影响 Windows 的客户端版本和服务器版本，包括 Vista 7、8.1、10、Server 2008、Server 2012 和 Server 2016。

MS16-150 修复了 Windows 安全内核模式中的一个权限提升漏洞 (CVE-2016-7271)。如果攻击者运行经特殊设计的应用，则其中最严重的漏洞可能导致权限提升。攻击如果成功，还可能破坏虚拟信任级别。该漏洞影响 Windows 10 和 Windows Server 2016。

MS16-151 修复了 Windows 内核模式驱动程序中的两个权限提升漏洞 (CVE-2016-7259、CVE-2016-7260)。如果攻击者运行经特殊设计的应用，则其中最严重的漏洞可能导致权限提升。该漏洞影响所有当前受支持的 Windows 版本。

MS16-152 修复了 Windows 内核中的一个信息泄露漏洞 (CVE-2016-7258)。当 Windows 内核不正确地处理内存中的特定对象时，该漏洞可能导致信息泄漏。该漏洞影响 Windows 10 和 Server 2016。

MS16-153 修复了 Windows 通用日志文件系统驱动程序中的一个信息泄露漏洞 (CVE-2016-7295)。当 Windows 内核不正确地处理内存中的特定对象时，该漏洞可能导致信息泄漏，攻击者运行经特殊设计的应用也可能会触发此漏洞。此漏洞影响所有当前受支持的 Windows 版本。

MS16-155 修复了 .NET Framework 中的一个信息泄露漏洞 (CVE-2016-7270)。此漏洞特别影响 .NET 4.6.2，并可能导致应受各种加密防护保护的信息泄露。此漏洞影响当前受支持的大多数 Windows 版本。

防护

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 SID：40647-40648、40936-40990 和 40992-40993

发布者：NICK BIASINI；发布时间：15:00

标签：CVE、MICROSOFT、星期二补丁、漏洞