2016 年 7 月 12 日，星期二

Microsoft 星期二补丁 - 2016 年 7 月

作者：William Largent

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 11 个公告修复了 49 个漏洞。在此次发布中，“严重”等级的公告有 6 个，分别修复了 Edge、Internet Explorer、JScript/VBScript、打印后台处理程序、Office 和 Adobe Flash Player 等产品中的漏洞。其余公告均为“重要”等级，分别修复了 Windows 内核、Office、内核模式驱动程序、.NET Framework 和安全启动中存在的漏洞。

评为严重等级的公告

在本次 Microsoft 发布中，公告 MS16-084 至 MS16-088 以及公告 MS16-093 被列为“严重”等级。

MS16-084 和 MS16-085 分别是本月关于 Internet Explorer 和 Edge 的安全公告。IE 安全公告修复了 Internet Explorer 版本 9、10 和 11 中的漏洞。IE 公告共涵盖 15 个漏洞，其中包括 9 个内存损坏漏洞、1 个安全功能绕过漏洞、3 个信息泄露漏洞和 2 个欺骗漏洞。Edge 公告共修复 13 个漏洞，其中包括 7 个内存损坏漏洞、1 个安全功能绕过漏洞、3 个信息泄露漏洞和 2 个欺骗漏洞。IE 漏洞在受影响的 Windows 客户端上被列为“严重”等级，但是在受影响的 Windows 服务器上仅列为“中等”等级。

MS16-086 修复了漏洞 CVE-2016-3204。这是一个内存损坏漏洞，是由于 Internet Explorer 中的 JScript 和 VBScript 引擎在内存中渲染对象的方式导致的。成功利用此漏洞的攻击者可获得与当前用户相同的权限，从而远程执行代码。攻击者可设法欺骗用户访问一个经特殊设计的网页，来触发此漏洞。

MS16-087 是本月关于 Microsoft 打印后台处理程序的公告，修复了 CVE-2016-3238 和 CVE-2016-3239 这两个漏洞。CVE-2016-3238 为打印后台处理程序服务漏洞，此打印后台处理程序服务在打印机安装过程中未正确地验证打印驱动程序。成功利用此漏洞的攻击者可远程执行任意代码。CVE-2016-3239 是一个本地特权提升漏洞。当打印后台处理程序服务器向底层文件系统执行写入时，便会存在此漏洞。要利用此漏洞，攻击者必须登录到受影响的系统，并运行经特殊设计的脚本或程序。

MS16-088 是本月关于 Microsoft Office 的公告，修复了 CVE-2016-3278 至 CVE-2016-3284 中列出的 7 个内存损坏漏洞。利用最严重的漏洞，攻击者可以在当前用户打开经特殊设计的文件后，获得与当前用户相同的权限，从而执行任意代码。攻击者可通过各种不同的方式发送经特殊设计的文件（如电子邮件），也可以将该文件托管在 Web 服务器上。此漏洞存在于 Microsoft Office 的多个版本中。

MS16-093 是有关 Adobe Flash Player 的安全更新，适用于 Microsoft Internet Explorer 10 和 11 以及 Microsoft Edge 中的 Flash Player 库。此安全更新修复了 24 个漏洞。有关这些漏洞的详情，可参阅 Adobe 安全公告 APSB16-25。

评为重要等级的公告

在本月的发布中，安全公告 MS16-089、MS16-090、MS16-091、MS16-092 和 MS16-094 被列为“重要”等级。

MS16-089 修复了 Windows 安全内核模式中的一个信息泄露漏洞 (CVE-2016-3256)。成功利用此漏洞的攻击者，可以获得对系统中的敏感信息的访问权限。利用此漏洞并结合其他漏洞，可以进一步危害您的系统。此安全更新适用于所有受支持的 Windows 10 版本。

MS16-090 修复了 Microsoft Windows 内核模式驱动程序中的多个漏洞。这些本地特权提升漏洞可能允许攻击者提升权限，攻击者可利用这些漏洞获得在内核模式下执行代码的权限。此安全更新适用于所有受支持的 Windows 版本。

MS16-091 修复了 CVE-2016-3255 漏洞。该漏洞是 .NET Framework 中的一个信息泄漏漏洞，与 .NET Framework 解析包含外部实体引用的 XML 输入的方式相关。攻击者可以通过利用经特殊设计的 XML 数据，获得读取任意文件的权限。此安全更新适用于多个版本的 .NET Framework。

MS16-092 修复了 Windows 内核中的多个漏洞。Windows 内核中存在一个漏洞，使攻击者有可能操纵位于低完整性安全级别应用外部的文件。攻击者需要利用其他漏洞，才能成功利用此漏洞 (CVE-2016-3258)。Windows 内核还存在一个信息泄漏漏洞，可能允许攻击者将信息从一个进程披漏到另一个进程。要利用此漏洞，攻击者需要获得本地系统访问权限，或者使用经特殊设计的应用 (CVE-2016-3272)。此安全更新适用于所有受支持的 Windows 版本。

MS16-094 是一个有关“安全启动”的安全更新，修复了 CVE-2016-3287 漏洞。安全启动中存在一个漏洞，可能允许对受影响的系统具有管理权限或物理访问权限的攻击者绕过安全启动的安全功能。攻击者可以通过绕过这些安全功能禁用代码完整性检查，从而能够在目标系统上加载经测试签名的可执行文件和驱动程序，并且/或者可以绕过 BitLocker 的安全启动完整性验证。此漏洞影响可所有受支持的 Windows 版本。

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 公告：39478-39487、39491-39496、39499-39525、39530-39531
Adobe 公告：39532-39559、39563-39566、39569-39572

发布者：EDMUND BRUMAGHIN；发布时间：19:43
标签：MICROSOFT、OFFICE、星期二补丁、SNORT 规则、WINDOWS