2017 年 6 月 13 日（星期二）

Microsoft 星期二补丁 - 2017 年 6 月

今天，Microsoft 发布了旨在修复漏洞的一系列月度安全更新。本月发布的安全更新可修复 92 个漏洞，其中 17 个为严重等级漏洞，75 个为重要等级漏洞。受影响的产品包括 Edge、Internet Explorer、Office、SharePoint、Skype for Business、Lync 和 Windows。

评为严重等级的漏洞

CVE-2017-0283

一种在 Windows Uniscribe 未正确处理内存中的对象时出现的远程代码执行漏洞。攻击者会通过这种攻击获得对受影响系统的全面控制。攻击者可通过诱使用户查看经特殊设计的网站或者打开经特殊设计的文件等多种手段对漏洞加以利用。

CVE-2017-0291/CVE-2017-0292

在用户打开经特殊设计的 PDF 文件时出现于 Microsoft Windows 中的两种远程代码执行漏洞。通过这种攻击，攻击者不仅可以在当前用户的上下文中执行任意代码，还可以通过让用户打开经特殊设计的 PDF 文件对漏洞加以利用。

CVE-2017-0294

一种在 Microsoft Windows 未能正确处理 cabinet 文件时出现的远程代码执行漏洞。攻击者可通过诱使用户打开经特殊设计的 cabinet 文件或欺诈网络打印机和用户将恶意 cabinet 文件当作打印机驱动程序安装对漏洞加以利用。

CVE-2017-8464

一种在 Windows Explorer 处理 LNK 文件时出现的远程代码执行漏洞。当系统显示经特殊设计的快捷方式的图标时即可能触发漏洞。

CVE-2017-8496/CVE-2017-8497

在 Microsoft Edge 浏览器错误访问内存中的对象时出现的两种远程代码执行漏洞。这种漏洞会造成内存损坏，这样攻击者可执行任意代码。攻击者可通过让用户访问经特殊设计的网站对漏洞加以利用。

CVE-2017-8499

在 Microsoft Edge JavaScript 脚本引擎未正确处理内存中的对象时出现的一种远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过让用户查看经特殊设计的网站来利用该漏洞。

CVE-2017-8517

Microsoft 浏览器的 JavaScript 引擎在未正确处理内存中的对象时出现的一种远程代码执行漏洞。攻击者可以通过经特殊设计的网站来利用该漏洞，从而获得对受影响的系统的全面控制。

CVE-2017-8520

一种存在于 Microsoft Edge JavaScript 脚本引擎中的远程代码执行漏洞，以处理内存对象的方式出现。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8522

一种远程代码执行漏洞，在处理 Microsoft 浏览器（包括 Internet Explorer 和 Edge）内存中的对象时以 JavaScript 引擎渲染的方式出现。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8524

Microsoft 浏览器 JavaScript 引擎在未正确处理内存中的对象时出现的一种远程代码执行漏洞。攻击者可以通过让用户查看经特殊设计的网站来利用该漏洞，从而获得与当前用户相同的用户权限。

CVE-2017-8527

在未正确处理经特殊设计的嵌入字体时出现于 Windows 字体库中的一种远程代码执行漏洞。攻击者可通过诱使用户查看经特殊设计的网站或者打开经特殊设计的文件等多种手段对漏洞加以利用。

CVE-2017-8528

一种在 Windows Uniscribe 未正确处理内存中的对象时出现的远程代码执行漏洞。攻击者可通过诱使用户查看经特殊设计的网站或者打开经特殊设计的文件等多种手段对漏洞加以利用。

CVE-2017-8543

一种在 Windows Search 未正确处理内存中的对象时出现的远程代码执行漏洞。攻击者可通过向 Windows Search 服务发送经特殊设计 SMB 消息对漏洞加以利用。

CVE-2017-8548/CVE-2017-8549

Microsoft 浏览器的 JavaScript 引擎在错误处理内存中的对象时出现的两种远程代码执行漏洞攻击者可通过诱使用户查看经特殊设计的网站来利用该漏洞。

评为重要等级的漏洞

CVE-2017-0173/CVE-2017-0215/CVE-2017-0216/CVE-2017-0218/CVE-2017-0219

存在于设备卫士中的几种安全功能绕过漏洞，攻击者可通过这些漏洞将恶意代码注入到 Windows PowerShell 会话中。拥有本地设备访问权限的攻击者可通过将恶意代码注入到代码完整性策略信任的脚本中来利用这些漏洞。

CVE-2017-0193

Windows Hyper-V 指令仿真在未能正确实施权限级别时出现的一种权限提升漏洞。该漏洞可与另一个漏洞配合使用以在运行时利用提升的权限。

CVE-2017-0260/CVE-2017-8506

在 Microsoft Office 加载动态链接库 (DLL) 文件前错误验证输入时出现的两种远程代码执行漏洞。攻击者可通过诱使用户打开经特殊设计的 Office 文档来利用这些漏洞，进而获得对受影响的系统的全面控制。

CVE-2017-0282/CVE-2017-0284/CVE-2017-0285

Windows Uniscribe 错误披露内存内容时出现的几种信息泄露漏洞。攻击者可通过诱使用户打开经特殊设计的文件或访问不受信任的网页来利用该漏洞。

CVE-2017-0286/CVE-2017-0287/CVE-2017-0288/CVE-2017-0289

Windows GDI 功能存在的几种信息泄露漏洞，可导致内存内容泄露。攻击者可通过诱使用户打开经特殊设计的文件或说服用户访问不受信任的网页来利用该漏洞。

CVE-2017-0295

一种存在于 Microsoft Windows 中的篡改漏洞，经过身份验证的攻击者可通过该漏洞修改 C:\Users\DEFAULT 文件夹结构。经过身份验证的用户通过先于目标用户在本地登录到计算机来利用该漏洞。此前登录到系统的用户不受此漏洞影响。

CVE-2017-0296

该漏洞是一种可影响 Windows 10 的权限提升漏洞。一种可能导致权限提升的缓冲区溢出漏洞。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-0297

一种在 Windows 内核未正确处理内存中的对象时出现的权限提升漏洞。本地攻击者可通过执行经特殊设计的应用来利用该漏洞，从而提升权限。

CVE-2017-0298

存在于 Windows 中的一种权限提升漏洞，尤其是在 Helppane.exe 中配置为以交互式用户身份运行的 DCOM 对象未能正确地对客户端进行验证时更可能出现该漏洞。在另一用户通过“终端服务”或“快速用户切换”登录到系统后，攻击者会登录到同一系统并执行将利用该漏洞的经特殊设计的应用，以此利用漏洞。

CVE-2017-0299/CVE-2017-0300/CVE-2017-8462

在 Windows 内核未正确初始化内存地址时出现的几种信息泄露漏洞。攻击者可通过这些漏洞检索信息，并可能绕过内核地址空间布局随机化 (KASLR)。攻击者可通过登录到受影响的系统并执行经特殊设计的应用对漏洞加以利用。

CVE-2017-8460

在用户打开经特殊设计的 PDF 文件时出现于 Microsoft Windows 中的一种信息泄露漏洞。攻击者可通过诱使用户打开经特殊设计的 PDF 文件来利用该漏洞。

CVE-2017-8465/CVE-2017-8466/CVE-2017-8468

几种可导致权限提升的释放后使用 (Use-After-Free) 型漏洞。尤其是在 Windows 未正确处理内存中的对象时更容易触发漏洞。攻击者可通过本地登录或说服用户执行经特殊设计的应用对这些漏洞加以利用。

CVE-2017-8469/CVE-2017-8470

在 Windows 内核错误初始化内存中的对象时出现的两种信息泄露漏洞。经过身份验证的攻击者可通过执行经特殊设计的应用来触发这些漏洞。

CVE-2017-8471/CVE-2017-8472/CVE-2017-8473/CVE-2017-8474/CVE-2017-8475/CVE-2017-8476/CVE-2017-8477/CVE-2017-8478/CVE-2017-8479/CVE-2017-8480/CVE-2017-8481/CVE-2017-8482/CVE-2017-8483/CVE-2017-8484/CVE-2017-8485/CVE-2017-8488/CVE-2017-8489/CVE-2017-8490/CVE-2017-8491/CVE-2017-8492/CVE-2017-8553

一种在 Windows 内核错误初始化内存中的对象时出现的信息泄露漏洞。经过身份验证的攻击者可通过执行经特殊设计的应用对漏洞加以利用。

CVE-2017-8493

一种在 Microsoft Windows 未能对某些变量执行大小写检查时出现的安全功能绕过漏洞。该漏洞会使攻击者可以设置只读或需要身份验证的变量。攻击者可通过执行经特殊设计的应用对漏洞加以利用，从而绕过 Windows 中的 UEFI 变量安全限制。

CVE-2017-8494

一种在 Windows 安全内核模式未正确处理内存中对象时出现的权限提升漏洞。在本地经过身份验证的攻击者可通过执行经特殊设计的应用对该漏洞加以利用。

CVE-2017-8507

一种在 Microsoft Outlook 解析经特殊设计的邮件消息时出现的远程代码执行漏洞。此漏洞会在 Microsoft Outlook 处理允许脚本执行的经特殊设计的消息时被触发。攻击者可通过诱使用户打开经特殊设计的邮件消息对该漏洞加以利用。

CVE-2017-8508

一种在 Microsoft Office 未正确处理文件格式解析时出现的安全功能绕过漏洞。漏洞本身不允许任意代码执行，但是它可以与另一漏洞配合使用以通过绕过安全功能来执行任意代码。攻击者可通过诱使用户打开经特殊设计的文件对漏洞加以利用。

CVE-2017-8509/CVE-2017-8510/CVE-2017-8511/CVE-2017-8512/CVE-2017-8513

一种在 Microsoft Office 未正确处理内存中的对象时出现的远程代码执行漏洞。攻击者在用户打开经特殊设计的文件时对漏洞加以利用。此文件可以通过电子邮件送达或托管于网站上。

CVE-2017-8514

一种 Microsoft SharePoint Server 未正确清理经特殊设计的请求时出现的反射型跨站点脚本漏洞。攻击者可通过向受影响的 SharePoint 服务器发送经特殊设计的请求对漏洞加以利用，并在当前用户的安全环境中运行该脚本。这种请求可以通过电子邮件或网站上经特殊设计的 URL 送达。

CVE-2017-8515

一种存在于 Microsoft Windows 中的拒绝服务漏洞，在未经身份验证的攻击者发送经特殊设计的核心模式请求时触发。此攻击会导致目标系统出现拒绝服务的情况，并需要重启才能解决。

CVE-2017-8519

一种在 Internet Explorer 未正确访问内存中的对象时出现的远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8521

一种存在于 Microsoft Edge JavaScript 脚本引擎中的远程代码执行漏洞，以处理内存对象的方式出现。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者可通过诱使用户访问经特殊设计的网页对漏洞加以利用。

CVE-2017-8523

一种 Microsoft Edge 未能正确针对出现在其他浏览器窗口的 HTML 要素应用同源策略时出现的安全功能绕过漏洞。在用户访问经特殊设计的网站时，攻击者可利用该漏洞诱骗用户访问带有恶意内容的页面。

CVE-2017-8529

该漏洞为针对 Internet Explorer 和 Edge 的信息泄露漏洞。漏洞尤其会出现在打印预览中，并可通过浏览到经特殊设计的 URL 触发。

CVE-2017-8530

一种 Microsoft Edge 未能正确执行同源策略时出现的安全功能绕过漏洞，攻击者可通过该漏洞从当前源以外的源访问信息。在用户访问经特殊设计的网站时，攻击者可利用该漏洞诱骗用户访问带有恶意内容的页面。

CVE-2017-8531/CVE-2017-8532/CVE-2017-8533

在 Windows GDI 错误披露内存内容时出现的几种信息披露漏洞。攻击者可通过诱使用户打开经特殊设计的文件或访问不受信任的网页，对漏洞加以利用。

CVE-2017-8534

一种在 Windows Uniscribe 错误披露内存内容时出现的信息泄露漏洞。攻击者可通过诱使用户打开经特殊设计的文件或访问不受信任的网页等多种方式对漏洞加以利用。

CVE-2017-8544

一种在 Windows Search 未正确处理内存对象时出现的信息泄露漏洞。攻击者可通过向 Windows Search 服务发送经特殊设计 SMB 消息对漏洞加以利用。

CVE-2017-8545

因为未正确清理或以安全的方式处理 HTML 而出现于 Mac 版 Microsoft Office 中的一种欺骗漏洞。攻击者可通过发送带有特殊 HTML 标签（显示恶意身份验证提示）的邮件利用该漏洞，从而可能获得用户身份验证信息或登录信息。

CVE-2017-8547

一种在 Internet Explorer 错误访问内存对象时出现的远程代码执行漏洞。该漏洞可能导致内存损坏，进而被利用以执行任意代码。攻击者通过诱使用户查看经特殊设计的网站，对漏洞加以利用。

CVE-2017-8550

一种远程代码执行漏洞，在 Skype 企业版和 Microsoft Lync Server 未能正确清理经特殊设计内容时出现。通过身份验证的攻击者可以利用此漏洞在 Skype 企业版或 Lync 环境中执行 HTML 和 Javascript 内容，例如：使用默认浏览器打开网页或开启与其他用户的消息会话。要利用该漏洞，攻击者需要邀请某位用户进行即时消息会话，然后发送含特殊设计的 Javascript 内容的信息。

CVE-2017-8551

一种在 SharePoint Server 未正确清理经特殊设计的网络请求时出现的权限提升漏洞。成功利用此漏洞的攻击者可能会对受影响的系统和在当前用户的安全环境下运行的脚本进行跨站脚本攻击。已验证的攻击者通过发送经特殊设计请求到受影响的 SharePoint Server，对该漏洞加以利用。

CVE-2017-8555

一种安全功能绕过漏洞，在 Microsoft Edge 未能正确验证 Edge 内容安全策略中的经特殊设计文件时出现。攻击者可利用该漏洞来诱骗用户加载包含恶意内容的网页。攻击者可通过诱导用户查看经特殊设计的网页对该漏洞加以利用。

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，请参阅管理中心或 Snort.org。

Snort 规则：
17042
24500
43155-43166
43169-43176

发布者：NICK BIASINI；发布时间：下午 4:48
标签：防护、Microsoft、微软周二补丁日、周二补丁日、Snort 规则