2017 年 5 月 9 日，星期二

Microsoft 星期二补丁 - 2017 年 5 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 56 个漏洞，其中 15 个为严重等级漏洞，41 个为重要等级漏洞。受影响的产品包括 .NET、DirectX、Edge、Internet Explorer、Office、SharePoint 和 Windows。

Talos 提供的服务除了覆盖常规的月度 Microsoft 安全公告，还覆盖了 Windows 中的 MsMpEng 恶意软件防护服务漏洞 CVE-2017-0290，该漏洞由 Google Project Zero 团队的 Natalie Silvanovich 和 Tavis Ormandy 报告。该特定漏洞的 Snort 规则 SID 为 42820-42821。

评为严重等级的漏洞

以下是 Microsoft 评为严重等级的漏洞：

- CVE-2017-0221
- CVE-2017-0222
- CVE-2017-0224
- CVE-2017-0227
- CVE-2017-0228
- CVE-2017-0229
- CVE-2017-0235
- CVE-2017-0236
- CVE-2017-0240
- CVE-2017-0266
- CVE-2017-0272
- CVE-2017-0277
- CVE-2017-0278
- CVE-2017-0279
- CVE-2017-0290

这些漏洞通过以下受影响的软件爆出。

Adobe Flash

Adobe 已发布适用于 Flash Player 的安全更新来修复内存损坏漏洞，这些漏洞一旦被利用可能会引发远程代码执行。由于在 Windows 8 和 10 中，Flash Player 已集成到 Internet Explorer 和 Edge 中，因此 Windows 受到这些漏洞的影响。有关详细信息，请点击此处参阅 Adobe 的 Flash Player 安全公告。

Internet Explorer/Edge

在 Internet Explorer、Edge 和这两个浏览器使用的脚本引擎组件中发现了多个内存损坏漏洞。出现这些漏洞是因为 Internet Explorer、Edge 和 Chakra（脚本引擎）处理内存中对象的方式存在问题。如果当前用户导航至经特殊设计的网页，攻击者可以在该用户的权限环境中，利用这些漏洞实现任意代码执行。

CVE：CVE-2017-0221、CVE-2017-0222、CVE-2017-0224、CVE-2017-0227、CVE-2017-0228、CVE-2017-0229、CVE-2017-0235、CVE-2017-0236、CVE-2017-0240、CVE-2017-0266

Windows SMB

在 Microsoft 服务器消息块 (SMB) 1.0 中发现了多个漏洞，攻击者可利用这些漏洞在目标主机上执行任意代码。根据 Microsoft 的公告，未经身份验证的攻击者可通过经特殊设计的数据包（传输到易受攻击的 SMBv1 服务器）利用这些漏洞。

CVE：CVE-2017-0272、CVE-2017-0277、CVE-2017-0278、CVE-2017-0279

Microsoft 恶意软件防护引擎

在 Microsoft 恶意软件防护引擎中发现了一个漏洞，此漏洞可能会在内核环境中引发任意代码执行。出现此漏洞 (CVE-2017-0290) 是因为恶意软件防护引擎对经特殊设计的文件进行了不当扫描。打开包含恶意文件的邮件、访问利用此漏洞的恶意网站，或者下载经特殊设计的恶意文件都可能让攻击者实现利用此漏洞的目的。

Microsoft 已在公告之外单独发布解决此问题的引擎更新。用户和管理员应当注意，恶意软件防护引擎的更新通常不需要执行任何操作，因为更新一般会在发布后 48 小时内自动应用。有关详细信息，请参阅 Microsoft 的安全公告。

评为重要等级的漏洞

以下是 Microsoft 评为重要等级的漏洞：

- CVE-2017-0064
- CVE-2017-0077
- CVE-2017-0171
- CVE-2017-0175
- CVE-2017-0190
- CVE-2017-0212
- CVE-2017-0213
- CVE-2017-0214
- CVE-2017-0220
- CVE-2017-0226
- CVE-2017-0230
- CVE-2017-0231
- CVE-2017-0233
- CVE-2017-0234
- CVE-2017-0238
- CVE-2017-0241
- CVE-2017-0242
- CVE-2017-0244
- CVE-2017-0245
- CVE-2017-0246
- CVE-2017-0248
- CVE-2017-0254
- CVE-2017-0255
- CVE-2017-0258
- CVE-2017-0259
- CVE-2017-0261
- CVE-2017-0262
- CVE-2017-0263
- CVE-2017-0264
- CVE-2017-0265
- CVE-2017-0267
- CVE-2017-0268
- CVE-2017-0269
- CVE-2017-0270
- CVE-2017-0271
- CVE-2017-0273

- CVE-2017-0274
- CVE-2017-0275
- CVE-2017-0276
- CVE-2017-0280
- CVE-2017-0281

这些漏洞通过以下受影响的软件爆出。

.NET

在 .NET Core 和 .NET Framework 中发现并修复了安全功能绕过漏洞。出现 CVE-2017-0248 是因为 .NET Core 和 .NET 组件未能完全验证证书。当攻击者提供不适用于特定用途但依然要用于该用途的证书时，就会利用此漏洞。

DirectX

发现并修复了 DirectX 图形内核子系统 (dxgkrnl.sys) 中的权限升级漏洞。出现 CVE-2017-0077 是因为内存中对象的处理方式不正确。如果用户运行的是经特殊编写且可利用此漏洞的应用，攻击者就有机会利用此漏洞。

Microsoft 浏览器

在 Microsoft Internet Explorer 和 Edge 中发现并修复了多个漏洞。其中，两个漏洞是 Edge 中的权限升级漏洞（CVE-2017-0233、CVE-2017-0241），一个是 IE 中的内存损坏漏洞 (CVE-2017-0226)，一个是 IE 中的安全功能绕过漏洞 (CVE-2017-0064)，一个是浏览器欺诈漏洞 (CVE-2017-0231)，还有一个是 ActiveX 信息披露漏洞 (CVE-2017-0242)。

Office

在 Mac 和 PC 版 Microsoft Office 中发现并修复了多个任意代码执行漏洞。出现这些漏洞是因为内存中对象的处理方式不正确，导致内存损坏以及当前权限级别环境下的任意代码执行。如果受害者在主机系统中使用易受攻击的 Office 版本打开经特殊设计的 Office 文档，攻击者就有机会利用这些漏洞。可能利用这些漏洞的攻击媒介包括基于邮件的攻击，在此类攻击中，用户要打开攻击者提供的恶意附件。

CVE：CVE-2017-0254、CVE-2017-0261、CVE-2017-0262、CVE-2017-0264、CVE-2017-0265、CVE-2017-0281

Sharepoint

在 Sharepoint Foundation 2013 中发现并修复了跨站点脚本 (XSS) 漏洞。出现 CVE-2017-0255 是因为不适当地清理了向受影响服务器发出的 Web 请求，从而可能让攻击者在当前用户环境中运行脚本。攻击者可以利用此漏洞读取敏感信息，或代表目标用户执行操作。

Win32k

在 Win32k 子系统中发现并修复了三个漏洞，攻击者可利用这些漏洞获得升级权限或获取关于系统的敏感信息。其中两个漏洞（CVE-2017-0246、CVE-2017-0263）为权限升级漏洞，而第三个漏洞 (CVE-2017-0245) 为信息披露漏洞，可能会泄露关于系统的敏感信息。出现这三个漏洞都是因为内核模式驱动程序未能正确处理内存中的对象，攻击者可能利用它们执行经特殊编写的应用。

Windows COM

在 Windows 组件对象模型 (COM) 中发现并修复了两个权限升级漏洞（CVE-2017-0213 和 CVE-2017-0214）。CVE-2017-0213 出现在 Windows COM Aggregate Marshaller 中是因为 COM Marshaller 处理接口请求的方式不正确。出现 CVE-2017-0214 是因为在加载库之前无法正确验证输入内容，攻击者可能在加载类型库时利用此漏洞。

Windows DNS

在 Windows DNS 服务器中发现并修复了拒绝服务漏洞 (CVE-2017-0171)。出现 CVE-2017-0171 是因为“当服务器配置为对版本查询进行应答时”，处理 DNS 查询的方式不正确。因此，远程攻击者可以利用此漏洞，导致主机无响应。

Windows GDI

在 Windows 图形设备接口 (GDI) 中发现并修复了信息披露漏洞，攻击者可利用该漏洞获取关于目标系统的信息。漏洞 (CVE-2017-0190) 本身不允许攻击者在目标系统上执行任意代码。但是，攻击者可将此漏洞与其他漏洞搭配使用来执行任意代码。

Windows Hyper-V

在 Windows Hyper-V 中发现并修复了权限升级漏洞。出现该漏洞 (CVE-2017-0212) 是因为主机服务器无法正确处理 vSMB 数据包。

Windows 内核

在 Windows 内核中发现并修复了五个漏洞，其中四个为信息披露漏洞，一个为权限升级漏洞。五个漏洞出现的原因均为内存中对象的处理方式不正确。

用户执行经过特殊编写的应用可能会让攻击者利用这些漏洞并获取进一步危害主机所需的信息（在出现信息披露漏洞时），或者获得升级权限来完全控制受影响的系统。请注意，对于权限升级漏洞 (CVE-2017-0244)，基于 x86-64 的系统会遭遇拒绝服务而不是权限升级。

CVE：CVE-2017-0175、CVE-2017-0220、CVE-2017-0244、CVE-2017-0258、CVE-2017-0259

Windows SMB

在 Microsoft 服务器消息块 (SMB) 1.0 中发现了多个漏洞，这些漏洞可在受影响主机上导致拒绝服务或信息泄露。出现这些漏洞是因为受影响主机处理 SMBv1 请求的方式不正确。

CVE：CVE-2017-0267、CVE-2017-0268、CVE-2017-0269、CVE-2017-0270、CVE-2017-0271、CVE-2017-0273、CVE-2017-0274、CVE-2017-0275、CVE-2017-0276、CVE-2017-0280

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：

- 42749-42785
- 42798-42799
- 42811-42812
- 42820-42821（适用于 CVE-2017-0290）

发布者：ALEXANDER CHIU；发布时间：20:28
标签：防护、星期二补丁、SNORT 规则