Microsoft 恶意软件防护引擎远程执行代码漏洞

安全预警通告

360安全监测与响应中心

2017 年 05 月 09 日

目录

第1章 安全通告

尊敬的客户：

2017 年 5 月 8 日微软公司官网发布安全公告更新 Microsoft Microsoft 恶意软件保护引擎。通知客户 Microsoft Microsoft 恶意软件保护引擎的更新解决了一个 Microsoft 恶意软件保护引擎的远程代码执行漏洞（CVE-2017-0290）。

该漏洞是由 Google Project Zero 的 Natalie Silvanovich 和 Tavis Ormandy 发现的。成功利用此漏洞的攻击者可在 LocalSystem 账户下执行任意代码，并控制系统。攻击者可以安装程序; 查看，更改或删除数据; 以及创建具有完整用户权限的新帐户。

目前该漏洞相关的细节和测试程序已经公开，该漏洞已经造成现实威胁。

360 安全监测与响应中心也将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 漏洞信息

2.1 漏洞描述

当 Microsoft 恶意软件保护引擎未正确扫描攻击者精心构造的文件导致内存损坏时，触发远程执行代码漏洞。成功利用此漏洞的攻击者可在 LocalSystem 账户下执行任意代码，并控制系统。攻击者可以安装程序；查看，更改或删除数据；甚至创建具有完整用户权限的新帐户。

要利用此漏洞，必须由受影响的 Microsoft 恶意软件防护引擎扫描特制的文件。攻击者可以通过多种方法将特制文件放置在 Microsoft 恶意软件防护引擎扫描的位置。例如，攻击者可以使用网站将特制文件传送到受害者的系统，当用户查看该网站的时候，这个特制的文件就会被 Microsoft 恶意软件防护引擎扫描。攻击者还可以通过电子邮件或在打开文件时扫描 Instant Messenger 消息中的特制文件。此外，攻击者可以利用提供托管用户内容的网站，将特制文件上传到由托管服务器上，Microsoft 恶意软件保护引擎就会在托管服务器上扫描攻击者提供的特制文件。

如果受影响的反恶意软件启用了实时保护，则 Microsoft 恶意软件保护引擎将自动扫描文件，从而在扫描特制文件时导致利用该漏洞。如果未启用实时扫描，则攻击者将需要等待直到发生计划扫描才能利用该漏洞。

2.2 风险等级

360 安全监测与响应中心风险评级为：危急

第3章 处置建议

3.1 确认影响范围

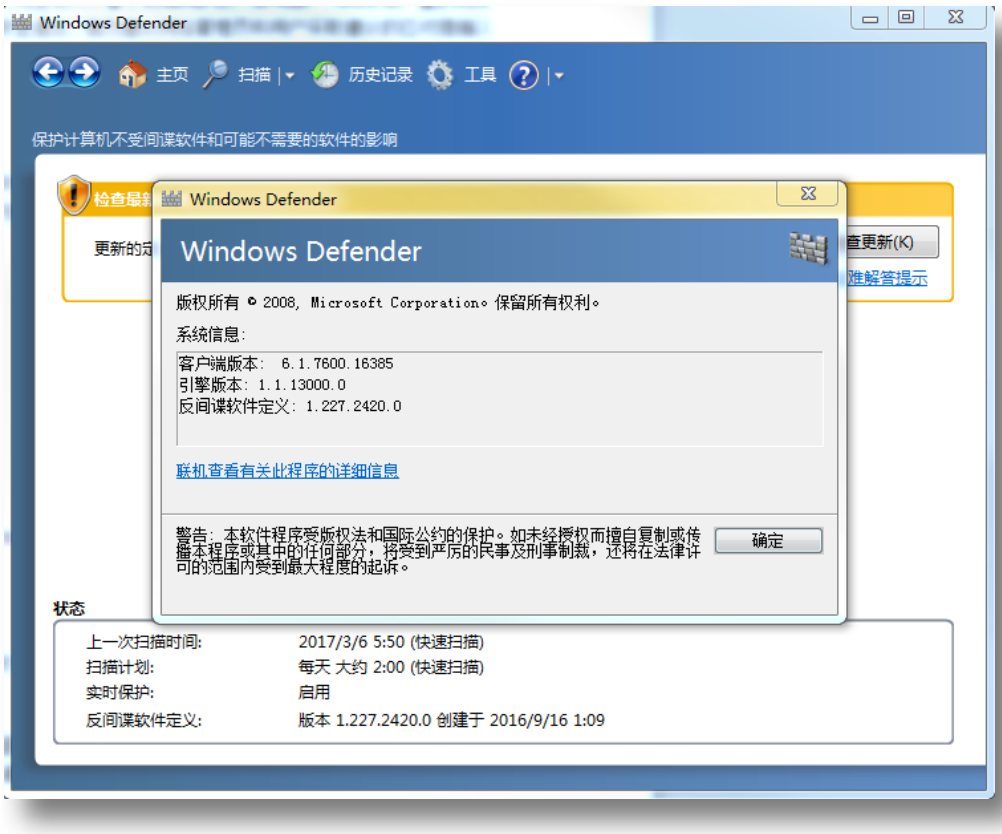
- Microsoft Forefront Endpoint Protection 2010
- Microsoft Endpoint Protection
- Microsoft Forefront Security for SharePoint Service Pack 3
- Microsoft System Center Endpoint Protection
- Microsoft Security Essentials
- Windows Defender for Windows 7
- Windows Defender for Windows 8.1
- Windows Defender for Windows RT 8.1
- Windows Defender for Windows 10, Windows 10 1511, Windows 10 1607, Windows Server 2016, Windows 10 1703
- Windows Intune Endpoint Protection

以上所有软件如果使用了 Microsoft Malware Protection Engine（mpengine.dll）版本小于等于 1.1.13701.0 ，则受此漏洞影响。

3.2 应急处置手段

点击 开始 按钮，在搜索框中输入 Windows Defender，点击出来的 Windows Defender 的图标，打开 Windows Defender 的控制面板，在上面的菜单中找到“关于 Windows Defender”。

Win7 系统中的界面如下：



Windows 10 系统中的界面如下：

其他 Windows 版本中的界面类似。检查“引擎版本”，如果其小于 1.1.13701.0，而且系统开启了 Windows Defender 服务，则当前系统受此漏洞影响。

如果系统安装了第三方病毒防护工具如 360 天擎，Windows Defender 会被关闭，此时则不受漏洞影响。

3.3 根治手段

检查是否安装更新，对于受影响的软件，请验证 Microsoft 恶意软件防护引擎版本是否为 1.1.13704.0 或更高版本。

如果必要的话，请安装更新。企业反恶意软件部署的管理员应确保其更新管理软件被配置为自动更新和部署，该更新会在 48 小时内生效。有关如何手动更新 Microsoft 恶意软件防护引擎和恶意软件定义的详细信息，请参阅 Microsoft 知识库文章 2510781。

3.4 快速应急处置建议

如果短期内无法更新 Windows Defender 系统，请在系统的服务管理器中关闭 Windows Defender 服务。

第4章 技术分析

4.1 整体影响评估

影响范围包括全部主要版本的 Windows 操作系统，对互联网部分和企业内网部分会产生重大影响。

4.2 可受影响区域

互联网区域、办公区域和内网（核心、业务）。

第5章 参考文档

漏洞详细信息可以参考如下链接：

https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5

https://technet.microsoft.com/en-us/library/security/4022344

http://m.bobao.360.cn/learning/detail/3826.html