# 安全漏洞通告

## Windows Installer 本地权限提升漏洞通告



360CERT
北京奇虎科技有限公司 | 2021-02-03

# 报告信息

| | | | |
|---|---|---|---|
| **报告名称** | Windows Installer 本地权限提升漏洞通告 | | |
| **报告类型** | 安全漏洞通告 | **报告编号** | B6-2021-020301 |
| **报告版本** | 1 | **报告日期** | 2021-02-03 |
| **报告作者** | 360CERT | **联系方式** | cert@360.cn |
| **提供方** | 北京奇虎科技有限公司 | | |
| **接收方** | | | |

# 报告修订记录

| 报告版本 | 日期 | 修订 | 审核 | 描述 |
|---|---|---|---|---|
| 1 | 2021-02-03 | 360CERT | 360CERT | 撰写报告 |

# 目录

# 一、 漏洞档案


| | |
|---|---|
| 漏洞类型 | 无类型 |
| CVE 编号 | 暂无 |
| 相关厂商 | microsoft |
| 相关组件 | microsoft |
| 威胁等级 | 高危 |
| 影响面 | 一般 |
| 360CERT 评分 | 8.5 |
| 修复方案 | 通用修补方案 |
| 漏洞发布时间 | 2021-02-03 |
| 报告生成时间 | 2021-02-03 |

## 二、 漏洞简述

360 安全卫士现已支持免疫该漏洞，建议用户更新 360 安全卫士到最新版缓解该漏洞影响 2021 年 02 月 03 日，360CERT 监测发现 Windows Installer 最新提权漏洞 EXP 已经在互联网公开，漏洞等级：高危，漏洞评分：8.5。

Windows Installler 在进行文件操作时存在一处漏洞，允许攻击者设置特殊的注册表项，进而提升权限到 SYSTEM(Windows 最高用户权限)。该漏洞为 CVE-2020-16902 的补丁绕过。

目前暂无补丁程序

对此，360CERT 建议广大用户好资产自查以及预防工作，以免遭受黑客攻击。

# 三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

| 评定方式 | 等级 |
| --- | --- |
| 威胁等级 | 高危 |
| 影响面 | 一般 |
| 360CERT 评分 | 8.5 |

## 四、 漏洞详情

在安装 MSI 程序包时，Windows Installer 会建立一个回滚脚本，以防安装失败时可以修复安装过程中进行了一系列修改。

但 Windows Installer 程序中存在漏洞，允许攻击者在安装过程中自定义回滚脚本的执行路径，进而导致 Windows 使用高权限执行该目标程序，完成权限提升。

攻击者可以通过修改 HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ services \ Fax \ ImagePath 的值为任意可执行文件路径如 c:\Windows\temp\evil.exe，这导致执行攻击者的 evil.exe 被执行。因为 Fax 服务的特性（高权限，任意用户可启动），借此完成权限提升。

# 五、 安全建议

## (一) 通用修补方案

1、安装病毒防护软件并升级病毒库

2、谨慎下载与打开互联网下载的文件

3、关注安全通告获得最新修补情况

# 六、 产品侧解决方案

## (一) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

# 七、 参考链接

1. Windows Installer Local Privilege Escalation 0day Gets a Micropatch

https://blog.0patch.com/2021/01/windows-installer-local-privilege.html

# 附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

| 严重 | |
|---|---|
| 评定标准 | 1. 9.0 ≤ 360CERT 评分 ≤ 10<br>2. Top20 组件<br>3. PoC/Exp 公开可直接利用<br>4. 获得系统权限<br>5. 蠕虫性攻击 |
| 危害结果 | 1. 任意攻击者可直接发起攻击<br>2. 直接获得服务器控制权限<br>3. 直接影响业务服务运行<br>4. 核心敏感数据泄漏<br>5. 下载任意文件<br>6. 易造成资金风险 |
| 修复建议 | 建议在 3 个工作日内对涉及的产品/组件进行修复操作 |

| 高危 | |
|---|---|
| 评定标准 | 1. 7.0 ≤ 360CERT 评分 < 9<br>2. 通用组件<br>3. PoC 公开<br>4. 获得服务/数据库权限 |
| 危害结果 | 1. 系统/服务/资源垂直越权<br>2. 获得数据库权限<br>3. 可造成资金风险 |
| 修复建议 | 建议在 7 个工作日内对涉及的产品/组件进行修复操作 |

| 中危 | |
|---|---|
| 评定标准 | 1. 4.0 ≤ 360CERT 评分 < 7<br>2. 需要额外的操作步骤方可实现攻击<br>3. 对服务的运行产生影响但不影响功能<br>a) 占用存储空间<br>b) 降低执行效率<br>4. 获得平台用户级权限 |
| 危害结果 | 1. 需要额外的操作步骤实现危害行为<br>2. 获得平台平行越权<br>3. 任意文件上传<br>4. 难造成资金风险 |
| 修复建议 | 建议在 12 个工作日内对涉及的产品/组件进行修复操作 |

| 低危 | |
|---|---|
| 评定标准 | 1. 0 ≤ 360CERT 评分 < 4<br>2. 不对服务的运行产生影响 |
| 危害结果 | 暂无 |
| 修复建议 | 建议在 20 个工作日内对涉及的产品/组件进行修复操作 |

# 附录 B 影响面说明

| 影响面说明 | |
|---|---|
| 广泛 | 影响主体数 > 10w<br>底层依赖库 |
| 一般 | 5w < 影响主体数 < 10w<br>开源库 |
| 局限 | 影响主体数 < 5w<br>特制版本的 |

# 附录 C 360 内部评分体系

**360 内部评分体系**是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

**360 内部评分体系**建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

| 分数 | 威胁等级 |
| --- | --- |
| 9.0 – 10.0 | 严重 |
| 7.0 – 8.9 | 高危 |
| 4.0 – 6.9 | 中危 |
| 0 - 3.9 | 低危 |