安全漏洞通告

【漏洞细节公开】CVE-2021-31985: Windows Defender 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	【漏洞细节公开】CVE-2021-31985: Windows Defender 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	
报告版本	1	报告日期	2021-07-08
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-07-08	360CERT	360CERT	撰写报告

目录

1 更新简介

1. Google Project Zero 于 07 月 08 日公开了该漏洞细节
2. **该漏洞无需用户交互，只要触发 Defender 对恶意文件的检测即可触发并利用漏洞**
3. 漏洞详情新增漏洞详细描述

2 漏洞简述

2021 年 07 月 08 日，360CERT 监测发现 GoogleProjectZero 发布了 CVE-2021-31985 的分析细节，漏洞等级：高危，漏洞评分：9.8。

Windows Defender 作为 Windows 的默认防线，其漏洞拥有极高的利用价值。因为默认可绕过 Windwos 系统防御机制，以及 Defender 本身以 SYSTEM（最高权限运行），该漏洞是 Defender 对历史格式 asprotect 的虚拟执行造成，攻击者可以通过向用户发送恶意邮件，该邮件自动触发 Defender 扫描邮件附件，攻击者借此即可接管用户计算机。

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。

3 风险等级

360CERT 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	广泛
攻击者价值	极高
利用难度	高
360CERT 评分	9.8

3.1 CVE-2021-31985: 代码执行漏洞

CVE: CVE-2021-31985

组件: Defender

漏洞类型: 代码执行

影响: 服务器接管

简述: Window Defender 在解析历史文件格式 asprotect 时采用了虚拟执行的方式，但由于解析过程中 Defender 以 SYSTEM（最高权限）允许，并且对执行过程的 DLL

加载未进行严格的校验，导致远程任意代码执行。攻击者构造特制的二进制程序，通过邮件等方式投递到用户计算机无需用户打开，即可接管用户计算机。同时该漏洞可绕过 Defender 的防御策略。

该漏洞无需用户交互，只要触发 Defender 对恶意文件的检测即可触发并利用漏洞

4 影响版本

组件	影响版本	安全版本
Windows:Defender	< 1.1.18200.3	>=1.1.18200.3

5 修复建议

5.1 通用修补建议

根据影响版本中的信息，排查并升级到安全版本

Windows 在 6 月补丁日已针对该漏洞发布修复程序，请用户开启 Window 自动更新以获得补丁安装。

360CERT 建议通过安装360 安全卫士进行一键更新。

应及时进行 Microsoft Windows 版本更新并且保持 Windows 自动更新开启。

Windows server / Windows 检测并开启 Windows 自动更新流程如下：

- 点击开始菜单，在弹出的菜单中选择“控制面板”进行下一步。
- 点击控制面板页面中的“系统和安全”，进入设置。
- 在弹出的新的界面中选择“windows update”中的“启用或禁用自动更新”。
- 然后进入设置窗口，展开下拉菜单项，选择其中的自动安装更新（推荐）。

6 时间线

2021-06-08 微软发布补丁日安全更新通告

2021-06-09 360CERT 发布通告

2021-07-08 GoogleProjectZero 公开漏洞详情

2021-07-08 360CERT 发布更新通告

7 参考链接

Issue 2189: mpengine: asprotect embedded runtime dll memory corruption

2021-06 补丁日：微软多个漏洞通告

CVE-2021-31985: Microsoft Defender Remote Code Execution Vulnerability

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn) 获取对应产品。

A.2 360 安全卫士

Windows 用户可通过 360 安全卫士实现对应补丁安装、漏洞修复、恶意软件查杀，其他平台的用户可以根据修复建议列表中的安全建议进行安全维护。
360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

A.3 360 安全卫士团队版

用户可以通过安装 360 安全卫士并进行全盘杀毒来维护计算机安全。360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

A.4 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.5 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

B 报告等级说明

360CERT 评分是依托于 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 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 实施攻击成本低，难度低 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 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 2. 通用组件 3. PoC 公开 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 2. 获得数据库权限 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 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 (a) 占用存储空间 (b) 降低执行效率 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 2. 获得平台平行越权 3. 任意文件上传 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 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

C 影响面说明

影响面说明	
广泛	1. 影响主体数 > 10w 2. 底层依赖库
一般	1. 5w < 影响主体数 < 10w 2. 次级开源库
局限	1. 影响主体数 < 5w 2. 特制版本的

D 360CERT 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