安全漏洞通告

CVE-2021-1647：Microsoft Defender 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-01-13

报告信息

报告名称	CVE-2021-1647：Microsoft 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**	B6-2021-011301
报告版本	1	**报告日期**	2021-01-13
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	2021-01-13	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	缓冲区/栈溢出漏洞
CVE 编号	CVE-2021-1647
相关厂商	Microsoft
相关组件	Microsoft Defender
威胁等级	高危
影响面	广泛
360CERT 评分	7.8
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-01-13
报告生成时间	2021-01-13

二、 漏洞简述

2021 年 01 月 13 日，360CERT 监测发现 Microsoft 发布了 Microsoft Defender 缓冲区/栈溢出漏洞 的风险通告，该漏洞编号为 CVE-2021-1647 ，漏洞等级：高危，漏洞评分：7.8。

攻击者通过 构造特殊的 PE 文件 ,可造成 Microsoft Defender 远程代码执行 。

该漏洞目前有在野利用

对此，360CERT 建议广大用户及时将 Microsoft Defender 升级到最新版本。与此同时，请做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	广泛
360CERT 评分	7.8

四、 漏洞详情

CVE-2021-1647: 缓冲区/栈溢出漏洞

攻击者通过构造特殊 PE 格式的文件，使得 Microsoft Defender 在对该文件进行解析的时候，产生缓冲区溢出，从而造成远程代码执行。

五、 影响版本

-Microsoft:Microsoft Defender:Windows 8.1 for 32-bit systems

-Microsoft:Microsoft Defender:Windows 7 for x64-based Systems Service Pack 1

-Microsoft:Microsoft Defender:Windows 7 for 32-bit Systems Service Pack 1

-Microsoft:Microsoft Defender:Windows Server 2016 (Server Core installation)

-Microsoft:Microsoft Defender:Windows Server 2016

-Microsoft:Microsoft Defender:Windows 10 Version 1607 for x64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1607 for 32-bit Systems

-Microsoft:Microsoft Defender:Windows 10 for x64-based Systems

-Microsoft:Microsoft Defender:Windows 10 for 32-bit Systems

-Microsoft:Microsoft Defender:Windows Server, version 20H2 (Server Core Installation)

-Microsoft:Microsoft Defender:Windows 10 Version 20H2 for ARM64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 20H2 for 32-bit Systems

-Microsoft:Microsoft Defender:Windows 10 Version 20H2 for x64-based Systems

-Microsoft:Microsoft Defender:Windows Server, version 2004 (Server Core installation)

-Microsoft:Microsoft Defender:Windows 10 Version 2004 for x64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 2004 for ARM64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 2004 for 32-bit Systems

-Microsoft:Microsoft Defender:Windows Server, version 1909 (Server Core installation)

-Microsoft:Microsoft Defender:Windows 10 Version 1909 for ARM64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1909 for x64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1909 for 32-bit Systems

-Microsoft:Microsoft Defender:Windows Server 2019 (Server Core installation)

-Microsoft:Microsoft Defender:Windows Server 2019

-Microsoft:Microsoft Defender:Windows 10 Version 1809 for ARM64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1809 for x64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1809 for 32-bit Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1803 for ARM64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1803 for x64-based Systems

-Microsoft:Microsoft Defender:Windows 10 Version 1803 for 32-bit Systems

-Microsoft:Microsoft System Center 2012 Endpoint Protection

-Microsoft:Microsoft Security Essentials

-Microsoft:Microsoft System Center 2012 R2 Endpoint Protection

-Microsoft:Microsoft System Center Endpoint Protection

-Microsoft:Microsoft Defender:Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

-Microsoft:Microsoft Defender:Windows Server 2008 for 32-bit Systems Service Pack 2

-Microsoft:Microsoft Defender:Windows RT 8.1

-Microsoft:Microsoft Defender:Windows 8.1 for x64-based systems

-Microsoft:Microsoft Defender:Windows Server 2012 R2 (Server Core installation)

-Microsoft:Microsoft Defender:Windows Server 2012 R2

-Microsoft:Microsoft Defender:Windows Server 2012 (Server Core installation)

六、 安全建议

(一) 通用修补方案

360CERT 建议通过安装

[360 安全卫士](http://weishi.360.cn/)

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） 。

(二) 临时修补方案

通过如下链接自行寻找符合操作系统版本的漏洞补丁，并进行补丁下载安装。

[2021 年 1 月安全更新 - 发行说明 - 安全更新程序指南 - Microsoft](https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan)

七、 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）。

八、 参考链接

1. Microsoft Defender Remote Code Execution Vulnerability

   https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1647

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 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. 任意攻击者可直接发起攻击 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

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 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