安全漏洞通告

Windows condrv.sys 本地拒绝服务漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-01-19

报告信息

报告名称	Windows condrv.sys 本地拒绝服务漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-011901
报告版本	1	**报告日期**	2021-01-19
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	2021-01-19	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	中危
影响面	一般
360CERT 评分	6.5
修复方案	通用修补方案
漏洞发布时间	2021-01-19
报告生成时间	2021-01-19

二、 漏洞简述

2021 年 01 月 19 日，360CERT 监测发现 @Jonas Lykkegaard 发布了 Windows condrv.sys 拒绝服务漏洞的风险通告，漏洞等级：中危，漏洞评分：6.5。

WIndows condrv.sys 组件存在一处逻辑漏洞，当本地用户向该组件传递特定的路径时会导致操作系统蓝屏，并拒绝服务。

condrv.sys 组件用于当开发者想要直接与 Windows 设备交互时，他们可以将 Win32 设备命名空间路径作为参数传递给各种 Windows 编程函数。例如，这允许应用程序直接与物理磁盘进行交互，而无需通过文件系统。

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	中危
影响面	一般
360CERT 评分	6.5

四、 漏洞详情

五、 安全建议

(一) 通用修补方案

1. 不访问不受信任的网站

2. 不要点击不明链接

3. 不要下载并执行未知文件

六、 产品侧解决方案

(一) 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。

(二) 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 10 bug crashes your PC when you access this location

https://www.bleepingcomputer.com/news/security/windows-10-bug-crashes-your-pc-when-you-access-this-location/

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