安全事件通告

Windows TCP/IP 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-02-10

报告信息

报告名称	Windows TCP/IP 远程代码执行漏洞通告		
报告类型	安全事件通告	**报告编号**	B6-2021-021001
报告版本	1	**报告日期**	2021-02-10
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	2021-02-10	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	代码执行
CVE 编号	CVE-2021-24074
相关厂商	Microsoft
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	9.8
修复方案	通用修补方案/临时修补方案
事件发布时间	2021-02-10
报告生成时间	2021-02-10

二、 事件简述

2021 年 02 月 10 日，360CERT 监测发现 微软 发布了 Windows TCP/IP 远程代码执行漏洞 的风险通告，该漏洞编号为 CVE-2021-24074 ，漏洞等级：严重，漏洞评分：9.8。

WIndows TCP/IP 协议中存在远程代码执行漏洞，攻击者通过精心构造的 IP 数据包，可直接在远程目标主机上执行任意代码。

对此，360CERT 建议广大用户及时将 windows 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、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.8

四、 事件详情

CVE-2021-24074: Windows TCP/IP 远程代码执行漏洞

WIndows TCP/IP 协议中存在远程代码执行漏洞，攻击者通过精心构造的 IP 数据包，可直接在远程目标主机上执行任意代码。该漏洞位于 IPv4 源路由中，默认情况下，系统会禁用此功能并拒绝相关请求。广大用户还可在防火墙及其它外围设备处设置源路由阻止策略。

五、 影响版本

产品名称	影响版本
windows	win7/win8/win10/server08/server12/server16/server19/server20H2

六、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-24074	代码执行	任意代码执行	严重

七、 安全建议

(一) 通用修补方案

通过如下链接寻找符合操作系统版本的漏洞补丁，并进行补丁下载安装。

[Windows TCP/IP Remote Code Execution Vulnerability](https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24074)

(二) 临时修补方案

1.将 sourceroutingbehavior 设置为“ drop”

netsh int ipv4 set global sourceroutingbehavior=drop

注意 ， 在 Windows 默认情况下，IPv4 源路由被认为是不安全的，系统将处理该来源请求并返回拒绝该请求的 ICMP 消息。但是，该解决方法将导致系统完全丢弃这些请求，而不进行任何处理。

若想撤销该变化，回到默认设置，请执行以下还原命令:

netsh int ipv4 set global sourceroutingbehavior=dontforward

2. 配置防火墙或负载平衡器以禁止源路由请求

八、 参考链接

1. Windows TCP/IP Remote Code Execution Vulnerability

   https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24074

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