关于微软 Windows 操作系统存在 TCP/IP 高危漏洞的预警通知

校属各单位：

2021 年 2 月 11 日，国家信息安全漏洞共享平台（CNVD）收录了两个微软 Windows 操作系统 TCP/IP 高危漏洞（CNVD-2021-10528，对应 CVE-2021-24074，CNVD-2021-10529，对应 CVE-2021-24086）。目前，漏洞细节尚未公开，微软已发布升级版本修复上述两个漏洞。

一、漏洞情况分析

2021 年 2 月 10 日，微软 Microsoft 在 2 月例行补丁日发布了 2 个 TCP/IP 高危漏洞（CVE-2021-24074/CVE-2021-24086）的补丁，这些漏洞影响绝大部分支持的 Windows 版本中的 TCP/IP 协议栈。

CVE-2021-24074 被标记为远程代码执行漏洞，出现此漏洞的原因由于两个数据包分片之间的 IPv4 选项字段错误，导致操作系统 IP 分片重新组装期间出现超出范围的读取和写入。攻击者可以通过构造特殊的 IP 源路由数据包触发漏洞，成功利用此漏洞的攻击者可能获得在目标服务器上执行任意代码的能力。

CVE-2021-24086 被标记为拒绝服务类型，攻击者可以通过发送多个精心制作的 IPv6 数据包（多个 IP 包头、无效包头、多个分片头等）触发漏洞，该漏洞利用成功可能导致目标主机发生蓝屏。

CNVD 对上述两个漏洞的综合评级为“高危”。

二、漏洞影响范围

根据微软官方公布的信息判断，上述两个漏洞几乎影响现有 Windows 操作系统的绝大部分版本，包括：

Windows 7 SP1-Windows10 20H2

Windows Server 2008-Windows Server 20H2

三、漏洞处置建议

经综合技术研判，由于上述两个漏洞的威胁程度高，范围广。攻击者如果成

功利用，可能导致受害组织内部信息系统瘫痪或失守。微软公司已发布了修复上述两个漏洞的安全补丁，CNVD 建议用户开启 Windows 自动更新程序进行自动修复，或者从微软官方下载补丁进行手动修复。

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

https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24086

https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb

附：参考链接：

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

https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24086

https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb

联系人：侯国平　　电话：65362000

信息技术中心

2021 年 2 月 19 日