网络安全风险预警通报

2020 年第 2 期 （总第 11 期）

广西大学网络信息中心 2023 年 8 月 12 日

【预警类型】 高危预警

【预警内容】

Windows DNS Server 存在远程代码执行漏洞的安全公告

安全公告编号 CNTA-2020-0015

一、漏洞概述

Microsoft Windows 是美国微软公司发布的视窗操作系统。DNS（DomainName Server，域名服务器）是进行域名和对应 IP 地址的转换服务器。DNS 中保存了域名与 IP 地址映射关系表，以解析消息的域名。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用细节已公开，微软公司已发布官方补丁。

二、漏洞详情

Windows DNS Server 远程代码执行漏洞。未经身份验证的攻击者利用该漏洞,向目标 DNS 服务器发送恶意构造请求,可以在目标系统上执行任意代码。由于该漏洞处于 Windows DNS Server 默认配置阶段即可触发,因此漏洞利用无需进行用户交互操作,存在被利用发起蠕虫攻击的可能。目前,已有公开渠道的漏洞利用模块发布,构成了蠕虫攻击威胁。

三、漏洞影响范围

漏洞影响的产品版本包括:

Windows Server 2008 for 32-bit SystemsService Pack 2

Windows Server 2008 for 32-bit SystemsService Pack 2 (Server Core installation)

Windows Server 2008 for x64-based SystemsService Pack 2

Windows Server 2008 for x64-based SystemsService Pack 2 (Server Core installation)

Windows Server 2008 R2 for x64-basedSystems Service Pack 1

四、漏洞处置建议

目前,微软官方已发布补丁修复此漏洞,CNVD 建议用户立即升级至最新版本:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

另可采取下列临时防护措施：

1、注册表项中添加 TcpReceivePacketSize 键值：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

DWORD = TcpReceivePacketSize

Value = 0xFF00

2、重新启动 DNS 服务。