河南省教育信息安全监测中心

Windows DNS 服务器远程代码执行漏洞

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2020 年 7 月 16 日

Windows DNS 服务器远程代码执行漏洞

事件描述

7 月 14 日，微软最新的月度补丁更新中修复了一枚存在于 Windows DNS 服务器中的可蠕虫化漏洞 CVE-2020-1350（代号 SigRed）。这意味着攻击者利用该漏洞能够在没有任何用户交互的情况下，在易受攻击的机器间传播，从而有可能感染整个组织的网络。

SigRed 漏洞源于 Windows DNS 服务器处理签名（SIG）记录查询的缺陷所致，超过 64 KB 的恶意 SIG 记录会导致堆缓冲区溢出，从而使攻击者能够远程执行具有高特权的代码，并远程接管易受攻击的服务器

漏洞编号

CVE-2020-1350

影响版本

Windows Server 2008 for 32-bit Systems Service Pack 2

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

Windows Server 2008 for x64-based Systems Service Pack 2

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

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Windows Server 2012

Windows Server 2012 (Server Core installation)

Windows Server 2012 R2

Windows Server 2012 R2 (Server Core installation)

Windows Server 2016

Windows Server 2016 (Server Core installation)

Windows Server 2019

Windows Server 2019 (Server Core installation)

Windows Server, version 1909 (Server Core installation)

Windows Server, version 1903 (Server Core installation)

Windows Server, version 2004 (Server Core installation)

安全建议

一、微软官方已针对受影响系统发布安全补丁，强烈建议相关用户尽快安装补丁更新。补丁升级，参考链接:

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

二、在应用补丁之前，建议将 DNS 消息（通过 TCP）的最大长度设置为 0xFF00 缓解漏洞。可以通过执行以下命令实现：

reg add “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters” /v “TcpReceivePacketSize” /t REG_DWORD /d 0xFF00 /f

net stop DNS && net start DNS

同时，建议设置 DNS 服务器为受信任的服务器。

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052