安全漏洞通告

2021-08 补丁日: 微软多个产品漏洞安全更新通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	2021-08 补丁日: 微软多个产品漏洞安全更新通告		
报告类型	安全漏洞通告	报告编号	B6-2021-081101
报告版本	1	报告日期	2021-08-11
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-08-11	360CERT	360CERT	撰写报告

目录

1 事件简述

2021 年 08 月 11 日，360CERT 监测发现 微软 发布了 8月份安全更新，事件等级：严重，事件评分：9.9。

此次安全更新发布了44个漏洞的补丁，主要覆盖了以下组件：Windows 操作系统、Microsoft Graphics Component、Remote Desktop Client、Windows NTLM、Windows TCP/IP、Windows Update Assistant 等。其中包含7个严重漏洞，37个高危漏洞。

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。

2 风险等级

360CERT 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
攻击者价值	高
利用难度	中
360CERT 评分	9.9

3 漏洞详情

3.1 CVE-2021-36948: Windows Update Medic Service 特权提升漏洞

CVE: CVE-2021-36948

组件: Windows Update Medic Service

漏洞类型: 特权提升

影响: 获得高等级用户权限；接管设备控制权限

3.2 CVE-2021-36936: Windows Print Spooler 代码执行漏洞

CVE: CVE-2021-36936

组件: Windows Print Spooler

漏洞类型: 代码执行

影响: 服务器接管

3.3 CVE-2021-36942: Windows LSA 欺骗攻击漏洞

CVE: CVE-2021-36942

组件: Windows LSA

漏洞类型: 欺骗攻击

影响: 用户身份窃取；获得高等级用户权限；接管设备控制权限

3.4 CVE-2021-34535: Windows Remote Desktop Client 代码执行漏洞

CVE: CVE-2021-34535

组件: Windows Remote Desktop Client

漏洞类型: 代码执行

影响: 服务器接管

3.5 CVE-2021-34530: Windows Graphics Component 代码执行漏洞

CVE: CVE-2021-34530

组件: Windows Graphics Component

漏洞类型: 代码执行

影响: 服务器接管

3.6 CVE-2021-26424: Windows TCP/IP 代码执行漏洞

CVE: CVE-2021-26424

组件: Windows TCP/IP

漏洞类型: 代码执行

影响: 服务器接管

4 影响版本

- Microsoft:Windows: [*]
- Microsoft:Windows10: [*]
- Microsoft:Windows7: [*]
- Microsoft:Windows8.1: [*]
- Microsoft:WindowsServer: [*]
- Microsoft:WindowsServer2008: [*]
- Microsoft:WindowsServer2012: [*]
- Microsoft:WindowsServer2016: [*]
- Microsoft:WindowsServer2019: [*]

5 修复建议

5.1 通用修补建议

360CERT 建议通过安装360 安全卫士进行一键更新。

应及时进行 Microsoft Windows 版本更新并且保持 Windows 自动更新开启。

Windows server / Windows 检测并开启 Windows 自动更新流程如下：

- 点击开始菜单，在弹出的菜单中选择"控制面板"进行下一步。
- 点击控制面板页面中的"系统和安全"，进入设置。
- 在弹出的新的界面中选择"windows update"中的"启用或禁用自动更新"。
- 然后进入设置窗口，展开下拉菜单项，选择其中的自动安装更新（推荐）。

5.2 临时修补建议

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。

August 2021 Security Updates

6 时间线

2021-08-10 微软发布安全更新

2021-08-11 360CERT 发布通告

7 参考链接

August 2021 Security Updates

THE AUGUST 2021 SECURITY UPDATE REVIEW

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 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获取对应产品。

A.2 360 安全卫士

Windows 用户可通过 360 安全卫士实现对应补丁安装、漏洞修复、恶意软件查杀，其他平台的用户可以根据修复建议列表中的安全建议进行安全维护。

360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

A.3 360 安全卫士团队版

用户可以通过安装 360 安全卫士并进行全盘杀毒来维护计算机安全。360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。

A.4 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.5 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。