安全事件通告

2021-06 补丁日：微软多个漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	2021-06 补丁日：微软多个漏洞通告		
报告类型	安全事件通告	报告编号	B6-2021-060901
报告版本	1	报告日期	2021-06-09
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	2021-06-09	360CERT	360CERT	撰写报告

目录

1 事件简述

2021 年 06 月 09 日，360CERT 监测发现 微软 发布了 6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50个漏洞的补丁，主要覆盖了以下组件：Windows 操作系统、Net Core、Office、Edge、SharePoint Server、Hyper-V、Visual Studio、Windows HTML Platform。其中包含5个严重漏洞，45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 漏洞详情

2.1 CVE-2021-33742: 代码执行漏洞

CVE: CVE-2021-33742

组件: Windows Trident

漏洞类型: 代码执行

影响: 服务器接管

简述: 已存在在野利用。MSHTML 的渲染引擎 Trident 中存在一处严重漏洞，攻击者可以通过构建特制的 Web 页面诱使用户访问，即可控制用户计算机设备。

2.2 CVE-2021-31201: 特权提升漏洞

CVE: CVE-2021-31201

组件: Enhanced Cryptographic Provider

漏洞类型: 特权提升

影响: 和其他漏洞组合下完全控制用户设备

简述: 已存在在野利用。该漏洞是加密程序中存在的一处本地权限提升漏洞，微软表示已发现该漏洞和 Adobe Reader CVE-2021-28550 组合进行远程利用。

2.3 CVE-2021-31199: 特权提升漏洞

CVE: CVE-2021-31199
组件: Enhanced Cryptographic Provider
漏洞类型: 特权提升
影响: 和其他漏洞组合下完全控制用户设备
简述: 已存在在野利用。该漏洞是加密程序中存在的一处本地权限提升漏洞，微软表示已发现该漏洞和 Adobe Reader CVE-2021-28550 组合进行远程利用。

2.4 CVE-2021-31956: 特权提升漏洞

CVE: CVE-2021-31956
组件: NTFS
漏洞类型: 特权提升
影响: 和其他漏洞组合下完全控制用户设备
简述: 已存在在野利用。该漏洞可造成的影响为本地权限提升，攻击者制作特制的二进制程序并诱使用户打开，即可控制用户计算机。

2.5 CVE-2021-33739: 特权提升漏洞

CVE: CVE-2021-33739
组件: DWM Core Library
漏洞类型: 特权提升

影响: 和其他漏洞组合下完全控制用户设备

简述: 已存在在野利用。攻击者通过构造特制的二进制文件并诱使用户打开，即可控制用户计算机。

2.6 CVE-2021-31968: 拒绝服务漏洞

CVE: CVE-2021-31968

组件: Remote Desktop Services

漏洞类型: 拒绝服务

影响: 无法远程桌面管理计算机

简述: 攻击者通过构造特制的 RDP 数据包发送至目标设备，可造成目标服务器宕机并停止服务。

2.7 CVE-2021-31985: 代码执行漏洞

CVE: CVE-2021-31985

组件: Defender

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者构造特制的二进制程序并诱使用户打开，即可接管用户计算机。该漏洞可绕过 Defender 的防御策略。

2.8 CVE-2021-31963: 代码执行漏洞

CVE: CVE-2021-31963

组件: SharePoint

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者通过构造特制的 Http 请求并发送至 SharePoint Server 即可接管该服务器。

3 影响版本

- Microsoft:DWMCoreLibrary: [*]
- Microsoft:Defender: [*]
- Microsoft:EnhancedCryptographicProvider: [*]
- Microsoft:RemoteDesktopServices: [*]
- Microsoft:SharePoint: [2019, 2013sp1, 2016]
- Microsoft:Windows: [*]
- microsoft:NTFS: [*]

4 修复建议

4.1 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）。

4.2 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。

June 2021 Security Updates

5 时间线

2021-06-08 微软发布通告

2021-06-09 360CERT 发布通告

6 参考链接

THE JUNE 2021 SECURITY UPDATE REVIEW

June 2021 Security Updates

A 产品侧解决方案

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。

A.2 360 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或 (shaoyulong#360.cn) 获取对应产品。

A.3 360 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.4 360 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.5 360 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.6 360 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。