安全漏洞通告

2021-05 补丁日：微软多个漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-05-12

报告信息

报告名称	2021-05 补丁日：微软多个漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-051201
报告版本	1	**报告日期**	2021-05-12
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-05-12	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	代码执行等
CVE 编号	CVE-2021-31166 等
相关厂商	microsoft
相关组件	microsoft
威胁等级	严重
影响面	广泛
360CERT 评分	9.9
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-05-12
报告生成时间	2021-05-12

二、 漏洞简述

2021 年 05 月 12 日，360CERT 监测发现 微软 发布了 5 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 55 个漏洞的补丁，主要覆盖了以下组件：Windows 操作系统、Exchange Server、.Net Core、Office、SharePoint Server、Hyper-V、Visual Studio。其中包含 4 个严重漏洞，50 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。

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	9.9

四、 漏洞详情

CVE-2021-31166: HTTP 协议远程代码执行漏洞

CVE: CVE-2021-31166

组件: HTTP Protocol

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者通过向主机发送特制流量包可触发该漏洞。该漏洞可以造成蠕虫级影响，可在可通信设备之间广泛传播。

CVE-2021-28476: Hyper-V 远程代码执行漏洞

CVE: CVE-2021-28476

组件: Hyper-V

漏洞类型: 代码执行

影响: 服务器接管

简述: 成功利用该漏洞的攻击者可以在 Hyper-V 的服务器上执行任意代码，并最终控制该服务器。

CVE-2021-27068: Visual Studio 远程代码执行漏洞

CVE: CVE-2021-27068

组件: Visual Studio

漏洞类型: 代码执行

影响: 服务器接管

简述: 成功利用该漏洞的攻击者可以通过 VS2019 在服务器上执行任意代码，并最终控制该服务器。该漏洞无需用户交互，且利用难度低。

CVE-2021-31204: .Net Core 权限提升漏洞

CVE: CVE-2021-31204

组件: .Net Core/Visual Studio

漏洞类型: 权限提升

影响: 获得服务器的高级控制权限

简述: 存在在野利用 .NET 5.0 以及 .NET Core 3.1 受到该漏洞影响，并同时影响 VS2019。成功利用该漏洞可实现低等级用户升级为高等级用户。

CVE-2021-31200: Common Utilites 远程代码执行漏洞

CVE: CVE-2021-31200

组件: Common Utilites

漏洞类型: 代码执行

影响: 服务器接管

简述: 存在在野利用 成功利用该漏洞可在服务器上执行任意代码，并最终控制该服务器。

CVE-2021-31207: Exchange Server 安全特性绕过漏洞

CVE: CVE-2021-31207

组件: Exchange Server

漏洞类型: 安全特性绕过

影响: 服务器控制

简述: 存在在野利用 该漏洞为 2021 Pwn2Own 上公开的漏洞，成功利用该漏洞可获得一定的服务器控制权限。

五、 安全建议

(一) 通用修补方案

360CERT 建议通过安装[360 安全卫士](http://weishi.360.cn/)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）。

(二) 临时修补方案

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。

[2021 年 05 月安全更新](https://msrc.microsoft.com/update-guide/releaseNote/2021-May)

六、 产品侧解决方案

(一) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。

(二) 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。

(三) 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。

七、 参考链接

1. Zero Day Initiative — The May 2021 Security Update Review

   https://www.zerodayinitiative.com/blog/2021/5/11/the-may-2021-security-update-review

2. May 2021 Security Updates - Release Notes - Security Update Guide - Microsoft

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

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危