安全漏洞通告

2021-04 补丁日: 微软多个高危漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-04-14

报告信息

报告名称	2021-04 补丁日: 微软多个高危漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-041402
报告版本	1	**报告日期**	2021-04-14
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	2021-04-14	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	代码执行
CVE 编号	CVE-2021-28480 等
相关厂商	microsoft
相关组件	暂无
威胁等级	严重
影响面	广泛
360CERT 评分	10.0
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-04-14
报告生成时间	2021-04-14

二、 漏洞简述

2021 年 04 月 14 日，360CERT 监测发现 Microsoft 官方发布了 4 月安全更新，事件等级：严重，漏洞评分：10。

此次安全更新发布了 114 个漏洞的补丁，主要覆盖了以下组件：Windows 操作系统、Exchange Server、Azure、Office、SharePoint Server、Hyper-V、 Visual Studio 和基于 Chromium 内核的 Edge。其中包含 19 个严重漏洞，88 个高危漏洞。

对此，360CERT 建议广大用户及时做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	10

四、 漏洞详情

CVE-2021-28480/CVE-2021-28481: Exchange Server 代码执行漏洞

CVE：CVE-2021-28480/CVE-2021-28481

组件：Exchange Server

漏洞类型：未授权远程代码执行

影响：服务器接管

简述：这两个漏洞都是未授权远程代码执行漏洞且不需要用户交互，根据微软官方补丁的描述，这两个漏洞可能造成蠕虫级漏洞的危害，其实际的危害程度高于微软 3 月补丁中修复的 Exchange 远程代码执行漏洞。

CVE-2021-28310: Win32k 特权提升漏洞

CVE：CVE-2021-28310

组件：win32k

漏洞类型：特权提升

影响：权限提升

简述：成功利用该漏洞的攻击者可以在目标系统上提升权限，根据微软官方的描述，该漏洞很可能已经出现了在野利用。

CVE-2021-28444: Windows Hyper-V 安全功能绕过漏洞

CVE：CVE-2021-28310

组件：Hyper-V

漏洞类型：中间人攻击

影响：截获流量修改数据包

简述：成功利用该漏洞的攻击者可以绕过 Hyper-V 上的 Router Guard 配置，将 Windows 配置为中间人路由器，最终可以截获流量并修改数据包。

多个运行时 RPC 调用远程代码执行漏洞

简述：本月补丁中有 27 个漏洞为此类漏洞，其中包括 12 个严重漏洞，15 个高危漏洞。成功利用这些漏洞的攻击者可以在另外一个用户的上下文中执行代码，并造成远程代码执行的效果

五、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-28480	代码执行	服务器接管	严重
CVE-2021-28481	代码执行	服务器接管	严重
CVE-2021-28310	特权提升	权限提升	严重
CVE-2021-28444	中间人攻击	截获流量修改数据包	严重

六、 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

通过如下链接自行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 04 月安全更新](https://msrc.microsoft.com/update-guide/releaseNote/2021-Apr)

七、 产品侧解决方案

(一) 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。

(二) 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）。

(三) 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。

八、 参考链接

1. 2021 年 04 月安全更新

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

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