漏洞分析报告

2020-12 补丁日: 微软多个高危漏洞通告

360CERT
北京奇虎科技有限公司 | 2020-12-09

报告信息

报告名称	2020-12 补丁日: 微软多个高危漏洞通告		
报告类型	漏洞分析报告	**报告编号**	B6-2020-120902
报告版本	1	**报告日期**	2020-12-09
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	2020-12-09	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	验证绕过漏洞
CVE 编号	CVE-2020-16996 等
相关厂商	Microsoft
相关组件	windows_server 等
威胁等级	严重
影响面	广泛
360CERT 评分	9.1
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2020-12-09
报告生成时间	2020-12-09

二、 漏洞简述

2020 年 12 月 09 日，360CERT 监测发现 微软官方 发布了 12 月安全更新 的风险通告，事件等级： 严重 ，事件评分： 9.8 。

此次安全更新发布了 58 个漏洞的补丁，主要涵盖了以下组件: Windows 操作系统、IE/Edge 浏览器、ChakraCore、Office 办公套件、Exchange Server、Azure、微软动态、Visual Studio 。其中包括 9 个严重漏洞，46 个高危漏洞。

对此，360CERT 建议广大用户及时将 Windows 操作系统及相关组件 升级到最新版本。与此同时，请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	9.1

四、 漏洞详情

CVE-2020-17132: 代码执行漏洞

由于 Exchange 对 cmdlet 参数的验证不正确，Microsoft Exchange 服务器中存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以在系统用户的上下文中运行任意代码。利用此漏洞需要拥有以某个 Exchange 角色进行身份验证的用户权限。该漏洞与`CVE-2020-16875`相似

CVE-2020-17121: 代码执行漏洞

SharePoint 中存在一处远程代码执行漏洞。经过身份验证的攻击者通过发送特制请求包，可在 SharePoint Web 应用中执行任意.NET 代码。

CVE-2020-16996: 验证绕过漏洞

Kerberos 验证流程中存在一处安全特性绕过漏洞。该漏洞影响 RBCD 流程，具体影响尚未公开。

CVE-2020-17095: 代码执行漏洞

Hyper-V 中存在一处代码执行漏洞，该漏洞可造成虚拟环境逃逸。远程攻击通过在 Hyper-V 虚拟环境中运行特制的二进制程序与宿主使用 vSMB 通信，可造成在宿主系统中执行任意代码。

五、 影响版本

产品名称	影响版本
windows_server	20H2/2012_r2/2012/2016/2019
windows	10_1607/10_1803/10_1809/10_2903/10_1909/20H2
windows_server	10_1607/10_1803/10_1809/10_2903/10_1909/20H2
windows_server	2016/2019
sharepoint_server	2016/2019
sharepoint_foundation	2010_sp2/2013_sp1
exchange_server	2016_cu17/2016_cu18
exchange_server	2019_cu6/2019_cu7
exchange_server	2013_cu23

六、 漏洞列表

已利用>易利用>可利用>难利用

编号	描述	新版可利用性	历史版本可利用性	公开状态	在野利用	导致结果
CVE-2020-17142	[严重]Microsoft Exchange 远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-17118	[严重]Microsoft SharePoint 远程代码执行漏洞	易利用	易利用	未公开	不存在	远程代码执行
CVE-2020-17131	[严重]Chakra 脚本引擎内存损坏漏洞	可利用	可利用	未公开	不存在	内存破坏
CVE-2020-17121	[严重]Microsoft SharePoint 远程代码执行漏洞	易利用	易利用	未公开	不存在	远程代码执行
CVE-2020-17095	[严重]Hyper-V 远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-17132	[严重]Microsoft Exchange 远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-17152	[严重]Microsoft Dynamics 365 for Finance and Operations（本地）远程代码执行漏洞	易利用	易利用	未公开	不存在	远程代码执行
CVE-2020-17158	[严重]Microsoft Dynamics 365 for Finance and Operations（本地）远程代码执行漏洞	易利用	易利用	未公开	不存在	远程代码执行
CVE-2020-17117	[严重]Microsoft Exchange 远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16996	[高危]Kerberos 安全功能绕过漏洞	可利用	可利用	未公开	不存在	

CVE-2020-17134	[高危]Windows Cloud Files Mini Filter Driver 特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17002	[高危]Azure SDK for C 安全功能绕过漏洞	可利用	可利用	未公开	不存在
CVE-2020-17122	[高危]Microsoft Excel 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-17097	[高危]Windows Digital Media Receiver 特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-16971	[高危]Azure SDK for Java 安全功能绕过漏洞	可利用	可利用	未公开	不存在
CVE-2020-17148	[高危]Visual Studio Code Remote Development 扩展程序远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-16962	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17129	[高危]Microsoft Excel 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-17144	[高危]Microsoft Exchange 远程代码执行漏洞	易利用	易利用	未公开	不存在 远程代码执行
CVE-2020-17159	[高危]Visual Studio Code Java 扩展程序包远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-17145	[高危]Azure DevOps Server 和 Team Foundation Services 欺骗漏洞	可利用	可利用	未公开	不存在 欺骗攻击
CVE-2020-17139	[高危]Windows 覆盖筛选器安全功能绕过漏洞	可利用	可利用	未公开	不存在
CVE-2020-17156	[高危]Visual Studio 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行

CVE-2020-17135	[高危]Azure DevOps Server 欺骗漏洞	可利用	可利用	未公开	不存在 欺骗攻击
CVE-2020-17130	[高危]Microsoft Excel 安全功能绕过漏洞	可利用	可利用	未公开	不存在
CVE-2020-17125	[高危]Microsoft Excel 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-17124	[高危]Microsoft PowerPoint 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-16964	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17123	[高危]Microsoft Excel 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-17092	[高危]Windows 网络连接服务权限提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17127	[高危]Microsoft Excel 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-16961	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17141	[高危]Microsoft Exchange 远程代码执行漏洞	可利用	可利用	未公开	不存在 远程代码执行
CVE-2020-17136	[高危]Windows Cloud Files Mini Filter Driver 特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17096	[高危]Windows NTFS 远程代码执行漏洞	易利用	易利用	未公开	不存在 远程代码执行
CVE-2020-16960	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17137	[高危]DirectX 图形内核特权提升漏洞	可利用	可利用	未公开	不存在 权限提升
CVE-2020-17099	[高危]Windows 锁屏安全功能绕过漏洞	可利用	可利用	未公开	不存在

CVE-2020-17103	[高危]Windows Cloud Files Mini Filter Driver 特权提升漏洞	可利用	可利用 未公开	不存在 权限提升
CVE-2020-16958	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用 未公开	不存在 权限提升
CVE-2020-17089	[高危]Microsoft SharePoint 特权提升漏洞	可利用	可利用 未公开	不存在 权限提升
CVE-2020-16959	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用 未公开	不存在 权限提升
CVE-2020-17160	[高危]Azure Sphere 安全功能绕过漏洞	可利用	可利用 未公开	不存在
CVE-2020-17150	[高危]Visual Studio Code 远程代码执行漏洞	可利用	可利用 未公开	不存在 远程代码执行
CVE-2020-17128	[高危]Microsoft Excel 远程代码执行漏洞	可利用	可利用 未公开	不存在 远程代码执行
CVE-2020-16963	[高危]Windows 备份引擎特权提升漏洞	可利用	可利用 未公开	不存在 权限提升

七、 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。

2020 年 12 月安全更新 - 发行说明 - 安全更新程序指南 - Microsoft:

https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec

八、 产品侧解决方案

(一) 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。

(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。

九、 参考链接

1. 2020 年 12 月安全更新 - 发行说明 - 安全更新程序指南 - Microsoft

   https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec

2. THE DECEMBER 2020 SECURITY UPDATE REVIEW

   https://www.thezdi.com/blog/2020/12/8/the-december-2020-security-update-review

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