安全事件通告

2020-10 补丁日: 微软多个产品高危漏洞安全风险通告

360CERT
北京奇虎科技有限公司 | 2020-10-14

报告信息

报告名称	2020-10 补丁日: 微软多个产品高危漏洞安全风险通告		
报告类型	安全事件通告	**报告编号**	B6-2020-101401
报告版本	1	**报告日期**	2020-10-14
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	2020-10-14	360CERT	360CERT	撰写报告

目录

一、事件档案

漏洞类型	代码执行漏洞
CVE 编号	
相关厂商	Microsoft
相关组件	
威胁等级	严重
影响面	广泛
360CERT 评分	10
修复方案	通用修补方案/临时修补方案
事件发布时间	2020-10-14
报告生成时间	2020-10-14

二、 事件简述

2020 年 10 月 14 日，360CERT 监测发现 微软官方 发布了 10 月份 的风险通告，事件等级：严重，事件评分：10。

此次安全更新发布了 87 个漏洞的补丁，主要涵盖了 Windows 操作系统、IE/Edge 浏览器、Office 组件及 Web Apps、Exchange 服务器、.Net 框架、Azure DevOps、Windows 编码解码器 。其中包括 11 个严重漏洞， 75 个高危漏洞。

本次安全更新存在`1 个`漏洞等级为`严重`且易利用的 WindowsTCP/IP 漏洞，以及存在`6 个`信息公开的漏洞

对此，360CERT 建议广大用户及时将 Windows 各项组件 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、 事件评级

经过安全技术人员的分析，最终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
360CERT 评分	10

四、 事件详情

CVE-2020-16898: Windows TCP/IP 远程代码执行漏洞

Windows TCP/IP 堆栈不当处理 ICMPv6 Router Advertisement 数据包时，存在一处远程执行代码漏洞。远程攻击者通过构造特制的数据包并发送到受影响的主机，成功利用此漏洞的攻击者可在目标主机上执行任意代码，并控制该主机。

CVE-2020-16947: Microsoft Outlook 远程代码执行漏洞

Microsoft Outlook 软件无法正确处理内存中的对象时，存在一处远程代码执行漏洞。远程攻击者通过构造特制的邮件内容发送到使用 Outlook 的用户，成功利用此漏洞的攻击者可在目标主机上执行任意代码，并控制该主机。

CVE-2020-16891: Windows Hyper-V 远程执行代码漏洞

Windows Hyper-V 无法正确验证虚拟操作系统上经身份验证的用户的输入时，存在一处远程执行代码漏洞。远程攻击者通过构造特制的二进制程序，并诱使用户在 Hyper-V 虚拟系统中打开，成功利用此漏洞的攻击者可在绕过 Hyper-V 在 Windows 主系统上执行任意代码，并控制该主机。

CVE-2020-16909: Windows 错误报告组件特权提升漏洞

Windows 错误报告 (WER)组件在处理和执行文件时，存在一处特权提升漏洞。远程攻击者通过构造特制的二进制程序，并诱使用户打开，成功利用此漏洞的攻击者可获得更高的用户权限，并控制该主机。微软标记该漏洞信息已经公开，ZDI 标识该漏洞已存在在野利用

五、 漏洞影响

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-2020-17003	[严重]Base3D 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-2020-16898	[严重]Windows TCP/IP 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-2020-16968	[严重]Windows 摄像头编解码器远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16951	[严重]Microsoft SharePoint 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-2020-16952	[严重]Microsoft SharePoint 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-2020-16915	[严重]Windows Media Foundation 组件损坏漏洞	可利用	可利用	未公开	不存在	内存破坏
CVE-2020-16891	[严重]Windows 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-2020-16967	[严重]Windows 摄像头编解码器远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16911	[严重]GDI 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-2020-16947	[严重]Microsoft Outlook 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-2020-16923	[严重]Microsoft 图形组件远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16885	[高危]Windows 存储 VSP 驱动程序特权提升漏洞	可利用	可利用	已公开	不存在	权限提升
CVE-2020-16908	[高危]Windows 安装程序特权提升漏洞	可利用	可利用	已公开	不存在	权限提升

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-2020-16937	[高危].NET Framework 信息泄漏漏洞	可利用	可利用	已公开	不存在	信息泄漏
CVE-2020-16909	[高危]Windows 错误报告组件特权提升漏洞	可利用	可利用	已公开	不存在	权限提升
CVE-2020-16938	[高危]Windows 内核信息泄漏漏洞	可利用	可利用	已公开	不存在	信息泄漏
CVE-2020-16901	[高危]Windows 内核信息泄漏漏洞	可利用	可利用	已公开	不存在	信息泄漏
CVE-2020-16946	[高危]Microsoft Office SharePoint	可利用	可利用	未公开	不存在	跨站脚本攻击
CVE-2020-16894	[高危]Windows NAT 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-2020-16886	[高危]PowerShellGet 模块 WDAC 安全功能绕过漏洞	可利用	可利用	未公开	不存在	
CVE-2020-16934	[高危]Microsoft Office 即点即用特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16955	[高危]Microsoft Office 即点即用特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16920	[高危]Windows 应用程序兼容性客户端库特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16976	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16944	[高危]Microsoft SharePoint Reflective	可利用	可利用	未公开	不存在	跨站脚本攻击
CVE-2020-16928	[高危]Microsoft Office 即点即用特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16900	[高危]Windows 事件系统特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16930	[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

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-2020-16877	[高危]Windows 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16913	[高危]Win32k 特权提升漏洞	易利用	易利用	未公开	不存在	权限提升
CVE-2020-16914	[高危]Windows GDI+ 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16921	[高危]Windows 文本服务框架信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-1167	[高危]Microsoft 图形组件远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16941	[高危]Microsoft SharePoint 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16995	[高危]适用于 Linux 的网络观察程序代理虚拟机扩展特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16933	[高危]Microsoft Word 安全功能绕过漏洞	可利用	可利用	未公开	不存在	
CVE-2020-1047	[高危]Windows Hyper-V 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16907	[高危]Win32k 特权提升漏洞	易利用	易利用	未公开	不存在	权限提升
CVE-2020-16922	[高危]Windows 欺骗漏洞	易利用	易利用	未公开	不存在	欺骗攻击
CVE-2020-16977	[高危]Visual Studio Code Python 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-2020-16974	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16942	[高危]Microsoft SharePoint 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16950	[高危]Microsoft SharePoint 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏

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-2020-16935	[高危]Windows COM Server 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16939	[高危]组策略特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-1243	[高危]Windows Hyper-V 拒绝服务漏洞	可利用	可利用	未公开	不存在	拒绝服务
CVE-2020-1080	[高危]Windows Hyper-V 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16940	[高危]Windows - User Profile Service 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16924	[高危]Jet 数据库引擎远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16897	[高危]NetBT 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16957	[高危] Windows Office 访问连接引擎远程代码执行漏洞	可利用	可利用	未公开	不存在	远程代码执行
CVE-2020-16904	[高危]Azure 功能特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16969	[高危]Microsoft Exchange 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16902	[高危]Windows 程序安装组件 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16912	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16954	[高危]Microsoft Office 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-2020-16905	[高危]Windows 错误报告组件特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16927	[高危]Windows 远程桌面协议(RDP) 拒绝服务漏洞	可利用	可利用	未公开	不存在	拒绝服务

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-2020-16975	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16899	[高危]Windows TCP/IP 拒绝服务漏洞	易利用	易利用	未公开	不存在	拒绝服务
CVE-2020-16910	[高危]Windows 安全功能绕过漏洞	可利用	可利用	未公开	不存在	
CVE-2020-0764	[高危]Windows 存储服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16918	[高危]Base3D 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-2020-16892	[高危]Windows 映像特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16887	[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-2020-16945	[高危]Microsoft Office SharePoint	可利用	可利用	未公开	不存在	跨站脚本攻击
CVE-2020-16953	[高危]Microsoft SharePoint 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16890	[高危]Windows 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-2020-16896	[高危]Windows 远程桌面协议(RDP) 信息泄漏漏洞	易利用	易利用	未公开	不存在	信息泄漏
CVE-2020-16948	[高危]Microsoft SharePoint 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16916	[高危]Windows COM Server 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16931	[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-2020-16876	[高危]Windows 应用程序兼容性客户端库特权提升漏洞	可利用	可利用	未公开	不存在	权限提升

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-2020-16972	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16929	[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-2020-16936	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16932	[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-2020-16889	[高危]Windows KernelStream 信息泄漏漏洞	可利用	可利用	未公开	不存在	信息泄漏
CVE-2020-16943	[高危]Dynamics 365 Commerce 特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16863	[高危]Windows 远程桌面服务拒绝服务漏洞	可利用	可利用	未公开	不存在	拒绝服务
CVE-2020-16973	[高危]Windows 备份服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升
CVE-2020-16980	[高危]Windows iSCSI 目标服务特权提升漏洞	可利用	可利用	未公开	不存在	权限提升

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。

October 2020 Security Updates: https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct

七、 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 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。

八、 参考链接

1. October 2020 Security Updates

   https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-Oct

2. Zero Day Initiative — The October 2020 Security Update Review

   https://www.thezdi.com/blog/2020/10/13/the-october-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高危度。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