漏洞事件报告

2021-01 补丁日: 微软多个高危漏洞通告

360CERT
北京奇虎科技有限公司 | 2021-01-13

报告信息

报告名称	2021-01 补丁日: 微软多个高危漏洞通告		
报告类型	漏洞事件报告	**报告编号**	B6-2021-011302
报告版本	1	**报告日期**	2021-01-13
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	2021-01-13	360CERT	360CERT	撰写报告

目录

一、 事件档案

漏洞类型	无类型
CVE 编号	CVE-2021-1647 等
相关厂商	Windows
相关组件	Windows 操作系统等
威胁等级	严重
影响面	广泛
360CERT 评分	8.8
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-01-12
报告生成时间	2021-01-13

二、 事件简述

2021 年 01 月 13 日，360CERT 监测发现 发布了 的风险通告，事件等级：严重，事件评分：8.8。

此次安全更新发布了 83 个漏洞的补丁，主要涵盖了以下组件: Windows 操作系统、Edge 浏览器、Office 办公套件、Windows 编解码器库、Visual Studio、SQL Server、反病毒引擎、.NET、Azure 。其中包括 10 个严重漏洞， 73 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、 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	8.8

四、 影响版本

编号	标题	导致结果
CVE-2021-1647	[严重]CVE-2021-1647 远程代码执行漏洞	远程代码执行
CVE-2021-1665	[严重]CVE-2021-1665 远程代码执行漏洞	远程代码执行
CVE-2021-1673	[严重]CVE-2021-1673 远程代码执行漏洞	远程代码执行
CVE-2021-1660	[严重]CVE-2021-1660 远程代码执行漏洞	远程代码执行
CVE-2021-1658	[严重]CVE-2021-1658 远程代码执行漏洞	远程代码执行
CVE-2021-1666	[严重]CVE-2021-1666 远程代码执行漏洞	远程代码执行
CVE-2021-1667	[严重]CVE-2021-1667 远程代码执行漏洞	远程代码执行
CVE-2021-1668	[严重]CVE-2021-1668 远程代码执行漏洞	远程代码执行
CVE-2021-1643	[严重]CVE-2021-1643 远程代码执行漏洞	远程代码执行
CVE-2021-1642	[高危]CVE-2021-1642 权限提升漏洞	权限提升
CVE-2021-1644	[高危]CVE-2021-1644 远程代码执行漏洞	远程代码执行
CVE-2021-1641	[高危]CVE-2021-1641 欺骗漏洞	欺骗
CVE-2021-1636	[高危]CVE-2021-1636 权限提升漏洞	权限提升
CVE-2021-1637	[高危]CVE-2021-1637 信息泄漏漏洞	信息泄漏
CVE-2021-1651	[高危]CVE-2021-1651 权限提升漏洞	权限提升
CVE-2021-1652	[高危]CVE-2021-1652 权限提升漏洞	权限提升
CVE-2021-1653	[高危]CVE-2021-1653 权限提升漏洞	权限提升

CVE-2021-1654	[高危]CVE-2021-1654	权限提升漏洞	权限提升
CVE-2021-1655	[高危]CVE-2021-1655	权限提升漏洞	权限提升
CVE-2021-1656	[高危]CVE-2021-1656	信息泄漏漏洞	信息泄漏
CVE-2021-1657	[高危]CVE-2021-1657	远程代码执行漏洞	远程代码执行
CVE-2021-1659	[高危]CVE-2021-1659	权限提升漏洞	权限提升
CVE-2021-1661	[高危]CVE-2021-1661	权限提升漏洞	权限提升
CVE-2021-1662	[高危]CVE-2021-1662	权限提升漏洞	权限提升
CVE-2021-1663	[高危]CVE-2021-1663	信息泄漏漏洞	信息泄漏
CVE-2021-1664	[高危]CVE-2021-1664	远程代码执行漏洞	远程代码执行
CVE-2021-1669	[高危]CVE-2021-1669	安全特性绕过漏洞	安全特性绕过
CVE-2021-1670	[高危]CVE-2021-1670	信息泄漏漏洞	信息泄漏
CVE-2021-1671	[高危]CVE-2021-1671	远程代码执行漏洞	远程代码执行
CVE-2021-1672	[高危]CVE-2021-1672	信息泄漏漏洞	信息泄漏
CVE-2021-1674	[高危]CVE-2021-1674	安全特性绕过漏洞	安全特性绕过
CVE-2021-1676	[高危]CVE-2021-1676	信息泄漏漏洞	信息泄漏
CVE-2021-1679	[高危]CVE-2021-1679	拒绝服务漏洞	拒绝服务
CVE-2021-1680	[高危]CVE-2021-1680	权限提升漏洞	权限提升
CVE-2021-1681	[高危]CVE-2021-1681	权限提升漏洞	权限提升
CVE-2021-1682	[高危]CVE-2021-1682	权限提升漏洞	权限提升

CVE-2021-1683	[高危]CVE-2021-1683	安全特性绕过漏洞	安全特性绕过
CVE-2021-1684	[高危]CVE-2021-1684	安全特性绕过漏洞	安全特性绕过
CVE-2021-1685	[高危]CVE-2021-1685	权限提升漏洞	权限提升
CVE-2021-1686	[高危]CVE-2021-1686	权限提升漏洞	权限提升
CVE-2021-1687	[高危]CVE-2021-1687	权限提升漏洞	权限提升
CVE-2021-1688	[高危]CVE-2021-1688	权限提升漏洞	权限提升
CVE-2021-1689	[高危]CVE-2021-1689	权限提升漏洞	权限提升
CVE-2021-1690	[高危]CVE-2021-1690	权限提升漏洞	权限提升
CVE-2021-1691	[高危]CVE-2021-1691	拒绝服务漏洞	拒绝服务
CVE-2021-1692	[高危]CVE-2021-1692	拒绝服务漏洞	拒绝服务
CVE-2021-1693	[高危]CVE-2021-1693	权限提升漏洞	权限提升
CVE-2021-1694	[高危]CVE-2021-1694	权限提升漏洞	权限提升
CVE-2021-1695	[高危]CVE-2021-1695	权限提升漏洞	权限提升
CVE-2021-1696	[高危]CVE-2021-1696	信息泄漏漏洞	信息泄漏
CVE-2021-1697	[高危]CVE-2021-1697	权限提升漏洞	权限提升
CVE-2021-1707	[高危]CVE-2021-1707	远程代码执行漏洞	远程代码执行
CVE-2021-1708	[高危]CVE-2021-1708	信息泄漏漏洞	信息泄漏
CVE-2021-1709	[高危]CVE-2021-1709	权限提升漏洞	权限提升
CVE-2021-1710	[高危]CVE-2021-1710	远程代码执行漏洞	远程代码执行

CVE-2020-26870	[高危]CVE-2020-26870	远程代码执行漏洞	远程代码执行
CVE-2021-1711	[高危]CVE-2021-1711	远程代码执行漏洞	远程代码执行
CVE-2021-1712	[高危]CVE-2021-1712	权限提升漏洞	权限提升
CVE-2021-1718	[高危]CVE-2021-1718	篡改漏洞	篡改
CVE-2021-1723	[高危]CVE-2021-1723	拒绝服务漏洞	拒绝服务
CVE-2021-1725	[高危]CVE-2021-1725	信息泄漏漏洞	信息泄漏
CVE-2021-1650	[高危]CVE-2021-1650	权限提升漏洞	权限提升
CVE-2021-1649	[高危]CVE-2021-1649	权限提升漏洞	权限提升
CVE-2021-1648	[高危]CVE-2021-1648	权限提升漏洞	权限提升
CVE-2021-1646	[高危]CVE-2021-1646	权限提升漏洞	权限提升
CVE-2021-1645	[高危]CVE-2021-1645	信息泄漏漏洞	信息泄漏
CVE-2021-1638	[高危]CVE-2021-1638	安全特性绕过漏洞	安全特性绕过
CVE-2021-1677	[高危]CVE-2021-1677	欺骗漏洞	欺骗
CVE-2021-1678	[高危]CVE-2021-1678	安全特性绕过漏洞	安全特性绕过
CVE-2021-1699	[高危]CVE-2021-1699	信息泄漏漏洞	信息泄漏
CVE-2021-1700	[高危]CVE-2021-1700	远程代码执行漏洞	远程代码执行
CVE-2021-1701	[高危]CVE-2021-1701	远程代码执行漏洞	远程代码执行
CVE-2021-1702	[高危]CVE-2021-1702	权限提升漏洞	权限提升
CVE-2021-1703	[高危]CVE-2021-1703	权限提升漏洞	权限提升

CVE-2021-1704	[高危]CVE-2021-1704	权限提升漏洞	权限提升
CVE-2021-1705	[中危]CVE-2021-1705	远程代码执行漏洞	远程代码执行
CVE-2021-1706	[高危]CVE-2021-1706	权限提升漏洞	权限提升
CVE-2021-1713	[高危]CVE-2021-1713	远程代码执行漏洞	远程代码执行
CVE-2021-1714	[高危]CVE-2021-1714	远程代码执行漏洞	远程代码执行
CVE-2021-1715	[高危]CVE-2021-1715	远程代码执行漏洞	远程代码执行
CVE-2021-1716	[高危]CVE-2021-1716	远程代码执行漏洞	远程代码执行
CVE-2021-1717	[高危]CVE-2021-1717	欺骗漏洞	欺骗
CVE-2021-1719	[高危]CVE-2021-1719	权限提升漏洞	权限提升

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 01 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/2021-Jan)

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）。

七、 参考链接

1. 2021 年 1 月安全更新

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

2. THE JANUARY 2021 SECURITY UPDATE REVIEW

   https://www.thezdi.com/blog/2021/1/12/the-january-2021-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