奇安信
新一代网络安全领军者

微软 1 月补丁日

多个产品高危漏洞

安全风险通告

奇安信 CERT

2021 年 01 月 13 日

目录

第 1 章 安全通告 1

第 2 章 文档信息 3

第 3 章 漏洞信息 4

3.1 漏洞描述 4
3.2 风险等级 6

第 4 章 处置建议 7

第 5 章 产品解决方案 8

5.1 奇安信天擎终端安全管理系统解决方案 8
5.2 奇安信天眼检测方案 8
5.3 奇安信网神网络数据传感器系统产品检测方案 8

第 6 章 参考资料 10

第1章 安全通告

尊敬的客户：

本月，微软共发布了 83 个漏洞的补丁程序，其中，Remote Procedure Call Runtime、Win32k、Microsoft Defender 等产品中的 10 个漏洞被微软官方标记为紧急漏洞。经研判，以下 9 个漏洞（包括 6 个紧急漏洞和 3 个重要漏洞）影响较大，如下表所示：

CVE 编号	风险等级	漏洞名称	利用可能
CVE-2021-1647	紧急	Microsoft Defender 远程代码执行漏洞	N/Y/D
CVE-2021-1658	紧急	RPC Runtime 远程代码执行漏洞	N/N/L
CVE-2021-1660	紧急	RPC Runtime 远程代码执行漏洞	N/N/L
CVE-2021-1666	紧急	RPC Runtime 远程代码执行漏洞	N/N/L
CVE-2021-1667	紧急	RPC Runtime 远程代码执行漏洞	N/N/L
CVE-2021-1673	紧急	RPC Runtime 远程代码执行漏洞	N/N/L
CVE-2021-1707	重要	Microsoft SharePoint Server 远程代码执行漏洞	N/N/M
CVE-2021-1709	重要	Windows Win32k 权限提升漏洞	N/N/M
CVE-2021-1674	重要	Windows Remote Desktop Protocol 核心安全特性绕过漏洞	N/N/L

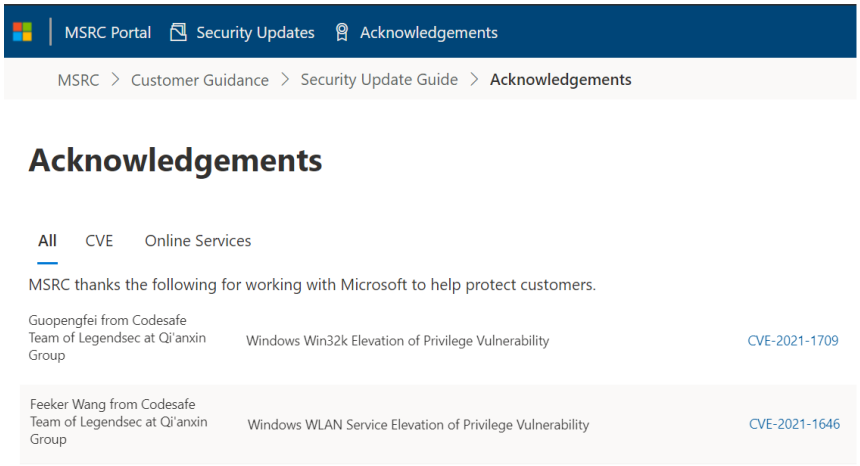
注：“利用可能”字段包含四个维度（是否公开[Y/N]/是否在野利用[Y/N]/可利用性评估[D/M/L/U/NA]）

简写	定义	翻译
Y	Yes	是
N	No	否
D	0-Exploitation detected	0-检测到利用
M	1-Exploitation more likely *	1-被利用可能性极大
L	2-Exploitation less likely **	2-被利用可能性一般
U	3-Exploitation unlikely ***	3-被利用可能性很小
NA	4-N/A	4-不适用

其中，CVE-2021-1647 Microsoft Defender 远程代码执行漏洞已发现在野利用，以下 2 个漏洞被微软标记为“Exploitation More Likely”，这代表这些漏洞更容易被利用：

- CVE-2021-1707
- CVE-2021-1709

以下漏洞由奇安信代码安全实验室发现并提交，包括：CVE-2021-1709、CVE-2021-1646。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。



奇安信 CERT 将持续关注该漏洞进展，并第一时间为您更新该漏洞信息。

第2章 文档信息

文档名称	微软 1 月补丁日多个产品高危漏洞安全风险通告
关键字	远程代码执行、权限提升
发布日期	2021 年 01 月 13 日
分析团队	奇安信 CERT

第3章 漏洞信息

3.1 漏洞描述

本月，微软共发布 83 个漏洞的补丁程序，其中，CVE-2021-1709、CVE-2021-1646 漏洞由奇安信代码安全实验室发现并提交。另外，CVE-2021-1647 Microsoft Defender 远程代码执行漏洞已发现在野利用，以下 2 个漏洞被微软标记为“Exploitation More Likely”，这代表这些漏洞更容易被利用：

- CVE-2021-1707
- CVE-2021-1709

奇安信 CERT 对此进行研判，影响较大的 9 个漏洞（包括 6 个紧急漏洞和 3 个重要漏洞）的详细信息如下：

1、CVE-2021-1647 Microsoft Defender 远程代码执行漏洞

漏洞名称	Microsoft Defender 远程代码执行漏洞				
漏洞类型	远程代码执行	**风险等级**	紧急	**漏洞 ID**	CVE-2021-1647
公开状态	未公开	**在野利用**	已发现		
漏洞描述	Microsoft Defender 中存在远程代码执行漏洞，攻击者可通过向目标受害者发送邮件或恶意链接等方式诱导受害者下载攻击者构造的恶意文件，从而使 Defender 在自动扫描时触发该漏洞，最终控制受害者计算机。据官方描述，CVE-2021-1647 目前已发现在野利用。Microsoft Malware Protection Engine 在最新版本中已更新补丁，用户联网可自动更新补丁。				
参考链接					
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647					

2、Remote Procedure Call Runtime 远程代码执行漏洞

漏洞名称	Remote Procedure Call Runtime 远程代码执行漏洞				
漏洞类型	远程代码执行	**风险等级**	紧急	**漏洞 ID**	详见漏洞描述
公开状态	未公开	**在野利用**	未发现		
漏洞描述	在 Windows 中 RPC（远程过程调用）开启时，存在五个远程代码执行漏洞（CVE-2021-1658、CVE-2021-1660、CVE-2021-1666、CVE-2021-1667、CVE-2021-1673），成功利用此漏洞需要网络访问权限及低特权的账户，利用难度较大。				
参考链接					
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1658 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1660 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1667 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1673					

3、CVE-2021-1707 Microsoft SharePoint Server 远程代码执行漏洞

漏洞名称	Microsoft SharePoint Server 远程代码执行漏洞				
漏洞类型	远程代码执行	**风险等级**	重要	**漏洞 ID**	CVE-2021-1707
公开状态	未公开	**在野利用**	未发现		
漏洞描述	Microsoft SharePoint 服务中存在远程代码执行漏洞（CVE-2021-1707），经过身份认证的攻击者可通过创建 SharePoint 网站来利用此漏洞，成功利用此漏洞的攻击者可在 SharePoint 应用程序池和 SharePoint 服务器账户的上下文中执行任意代码。				
参考链接					
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1707					

4、CVE-2021-1709 Windows Win32k 权限提升漏洞

漏洞名称	Windows Win32k 权限提升漏洞				
漏洞类型	权限提升	**风险等级**	重要	**漏洞 ID**	CVE-2021-1709
公开状态	未公开	**在野利用**	未发现		
漏洞描述	Win32k 存在一个权限提升漏洞。经过本地身份验证的攻击者可利用此漏洞在目标系统上以完全用户权限执行任意代码。				
参考链接					
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1709					

5、CVE-2021-1674 Windows Remote Desktop Protocol 核心安全特性绕过漏洞

漏洞名称	Windows Remote Desktop Protocol 核心安全特性绕过漏洞				
漏洞类型	安全特性绕过	**风险等级**	重要	**漏洞 ID**	CVE-2021-1674
公开状态	未公开	**在野利用**	未发现		
漏洞描述	Windows 远程桌面协议（RDP）中存在安全功能绕过漏洞，具有低特权帐户和网络访问权限的攻击者可以进行利用，目前尚无更多细节。				
参考链接					
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1674					

3.2 风险等级

奇安信 CERT 风险评级为：高危

风险等级：蓝色（一般事件）

第4章 处置建议

使用奇安信天擎的客户可以通过奇安信天擎控制台一键更新修补相关漏洞，也可以通过奇安信天擎客户端一键更新修补相关漏洞。

也可以采用以下官方解决方案及缓解方案来防护此漏洞：

Windows 自动更新

Windows 系统默认启用 Microsoft Update，当检测到可用更新时，将会自动下载更新并在下一次启动时安装。还可通过以下步骤快速安装更新：

1、点击“开始菜单”或按 Windows 快捷键，点击进入“设置”

2、选择“更新和安全”，进入“Windows 更新”（Windows 8、Windows 8.1、Windows Server 2012 以及 Windows Server 2012 R2 可通过控制面板进入“Windows 更新”，步骤为“控制面板”-> “系统和安全”->“Windows 更新”）

3、选择“检查更新”，等待系统将自动检查并下载可用更新

4、重启计算机，安装更新

系统重新启动后，可通过进入“Windows 更新”->“查看更新历史记录”查看是否成功安装了更新。对于没有成功安装的更新，可以点击该更新名称进入微软官方更新描述链接，点击最新的 SSU 名称并在新链接中点击“Microsoft 更新目录”，然后在新链接中选择适用于目标系统的补丁进行下载并安装。

手动安装补丁

另外，对于不能自动更新的系统版本（如 Windows 7、Windows Server 2008、Windows Server 2008 R2），可参考以下链接下载适用于该系统的 1 月补丁并安装：

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

第5章 产品解决方案

5.1 奇安信天擎终端安全管理系统解决方案

奇安信天擎终端安全管理系统并且有漏洞修复相关模块的用户，可以将补丁库版本更新到：2021.01.13.1 及以上版本，对内网终端进行补丁更新。

推荐采用自动化运维方案，如果控制中心可以连接互联网的用户场景，建议设置为自动从奇安信云端更新补丁库至 2021.01.13.1 版本。

控制中心补丁库更新方式：每天 04:00-06:00 自动升级，升级源为从互联网升级。

纯隔离网内控制中心不能访问互联网，不能下载补丁库和补丁文件，需使用离线升级工具定期导入补丁库和文件到控制中心。

5.2 奇安信天眼检测方案

奇安信天眼新一代安全感知系统已经能够有效检测针对该漏洞的攻击，请将规则版本升级到 3.0.0113.12585 或以上版本。规则 ID 及规则名称：

0x5d93, Microsoft Windows Defender 远程代码执行漏洞(CVE-2021-1647);

0x10020BAC, Microsoft SharePoint Server 远程执行代码漏洞(CVE-2021-1707);

奇安信天眼流量探针规则升级方法：系统配置->设备升级->规则升级，选择“网络升级”或“本地升级”。

5.3 奇安信网神网络数据传感器系统产品检测方案

奇安信网神网络数据传感器（NDS3000/5000/9000 系列）产品，已具备该补丁日多个高危漏洞（含 Microsoft Defender 远程代码执行漏洞(CVE-2021-1647)、Microsoft SharePoint Server 远程代码执行漏洞(CVE-2021-1707)）的检测能

力。对应的规则 ID 为：6117、6116，建议用户尽快升级检测规则库至 2101131422 以后版本并启用该多个检测规则。

第6章 参考资料

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

奇安信 CERT

【我们是谁】

奇安信应急响应部（又称：奇安信 CERT，奇安信 A-TEAM）成立于 2016 年，是属于奇安信旗下的网络安全应急响应平台，平台旨在第一时间为客户提供漏洞或网络安全事件安全风险通告、响应处置建议、相关技术和奇安信相关产品的解决方案。

奇安信 A-TEAM：团队主要致力于 Web 渗透、APT 攻防、对抗，前瞻性攻防工具预研。从底层原理、协议层面进行严肃、有深度的技术研究，深入还原攻与防的技术本质，曾多次率先披露 Windows 域、Exchange、WebLogic、Exim 等重大安全漏洞，第一时间发布相关漏洞风险通告及可行的处置措施并获得官方致谢。欢迎有意者加入！

【我们的服务】

安全风险通告：奇安信 CERT 成立至今已发布上百篇安全风险通告，从成立至今，针对多个高危漏洞、网络安全事件发布风险通告并给出了有效的安全措施。我们的安全研究团队将实时跟踪安全热点事件和漏洞，始终站在用户的视角去评估风险，致力于第一时间向客户发送有效的风险和相关解决方案。

【订阅方式】

发送接收邮箱和所属单位至：

cert@qianxin.com

【微信公众号】

奇安信 CERT