北京师范大学网络信息安全通告

2020年6月报告

北京师范大学信息网络中心

2020 年 7 月

目录

漏洞态势 2
1. 公开漏洞情况 2
1.1. 漏洞增长概况 2
1.2. 漏洞分布情况 3
1.2.1. 漏洞厂商分布 3
1.2.2. 漏洞产品分布 3
1.2.3. 漏洞类型分布 4
1.2.4. 漏洞危害等级分布 5
1.3. 漏洞修复情况 6
1.3.1. 整体修复情况 6
1.3.2. 厂商修复情况 6
1.4. 重要漏洞实例 7
1.4.1. 超危漏洞实例 7
1.4.2. 高危漏洞实例 15
2. 接报漏洞情况 28
3. 重大漏洞预警 31
3.1. 微软多个安全漏洞的预警 31
3.2. IBM WebSphere Application Server 远程代码执行漏洞的预警 37

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2020 年 6 月份新增安全漏洞共 1685 个，从厂商分布来看，Microsoft 公司产品的漏洞数量最多，共发布 130 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 13.35%。本月新增漏洞中，超危漏洞 177 个、高危漏洞 667 个、中危漏洞 795 个、低危漏洞 46 个，相应修复率分别为 83.62%、88.16%、84.65%以及 76.09%。合计 1444 个漏洞已有修复补丁发布，本月整体修复率 85.70%。

截至 2020 年 06 月 30 日，CNNVD 采集漏洞总量已达 147141 个。

1.1 漏洞增长概况

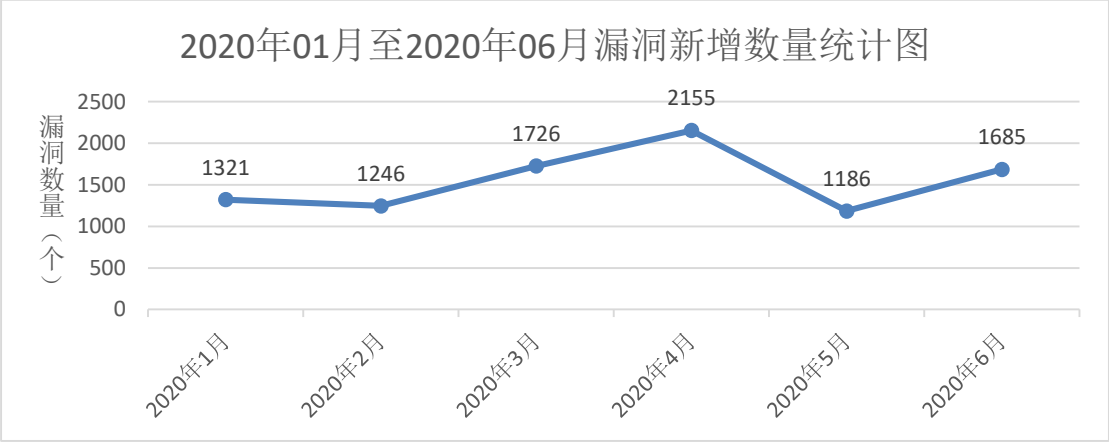

图 1 2020 年 1 月至 2020 年 6 月漏洞新增数量统计图

2020 年 6 月新增安全漏洞 1685 个，与上月（1186 个）相比增加了 42.07%。根据近 6 个月来漏洞新增数量统计图，平均每月漏洞数量达到 1553 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

6 月厂商漏洞数量分布情况如表 1 所示，Google 公司漏洞达到 135 个，占本月漏洞总量的 8.01%。

表 1　2020 年 6 月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量	所占比例
1	Google	135	8.01%
2	Microsoft	130	7.72%
3	Cisco	89	5.28%
4	IBM	65	3.86%
5	Foxit	48	2.85%
6	Adobe	36	2.14%
7	Atlassian	32	1.90%
8	Intel	25	1.48%
9	Qualcomm	23	1.36%
10	Linux 基金会	22	1.31%

1.2.2 漏洞产品分布

6 月主流操作系统的漏洞统计情况如表 2 所示。本月 Android 漏洞数量最多，共 110 个，占主流操作系统漏洞总量的 18.97%，排名第一。

表 2　2020 年 6 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Android	110
2	Windows 10	93
3	Windows Server 2019	80

4	Windows Server 2016	57
5	Windows 8.1	34
6	Windows Server 2012	34
7	Windows Rt 8.1	34
8	Windows Server 2012 R2	34
9	Windows Server 2008	31
10	Windows Server 2008 R2	31
11	Windows 7	30
12	Linux Kernel	12
13	Apple Mac OS	0

*由于 Windows 整体市占率高达百分之九十以上，所以上表针对不同的 Windows 版本分别进行统计

*上表漏洞数量为影响该版本的漏洞数量，由于同一漏洞可能影响多个版本操作系统，计算某一系列操作系统漏洞总量时，不能对该系列所有操作系统漏洞数量进行简单相加。

1.2.3 漏洞类型分布

6 月份发布的漏洞类型分布如表 3 所示，其中缓冲区错误类漏洞所占比例最大，约为 13.35%。

表 3 2020 年 6 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	缓冲区错误	225	13.35%
2	跨站脚本	172	10.21%
3	输入验证错误	132	7.83%
4	信息泄露	113	6.71%
5	代码问题	96	5.70%
6	资源管理错误	67	3.98%
7	授权问题	47	2.79%
8	跨站请求伪造	31	1.84%
9	信任管理问题	30	1.78%
10	路径遍历	29	1.72%
11	SQL 注入	28	1.66%
12	操作系统命令注入	25	1.48%
13	注入	24	1.42%
14	访问控制错误	22	1.31%
15	数据伪造问题	15	0.89%

16	命令注入	11	0.65%
17	权限许可和访问控制问题	9	0.53%
18	加密问题	8	0.47%
19	代码注入	8	0.47%
20	后置链接	7	0.42%
21	环境问题	6	0.36%
22	竞争条件问题	5	0.30%
23	日志信息泄露	5	0.30%
24	安全特征问题	3	0.18%
25	数字错误	2	0.12%
26	参数注入	1	0.06%
27	格式化字符串错误	1	0.06%
28	处理逻辑错误	0	0.00%
29	默认配置问题	0	0.00%
30	配置错误	0	0.00%
31	调试信息泄露	0	0.00%
32	其他	563	33.41%

1.2.4 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。6 月漏洞危害等级分布如图 2 所示，其中超危漏洞 177 条，占本月漏洞总数的 10.50%。

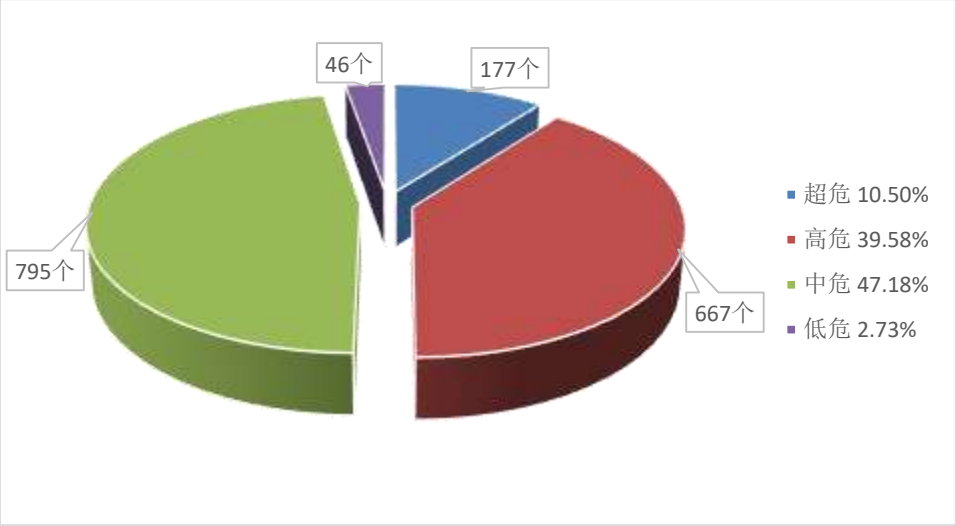

图 2　2020 年 6 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

6 月漏洞修复情况按危害等级进行统计见图 3。其中高危漏洞修复率最高，达到 88.16%，低危漏洞修复率最低，比例为 76.09%。总体来看，本月整体修复率，由上月的 86.09%下降至本月的 85.70%。

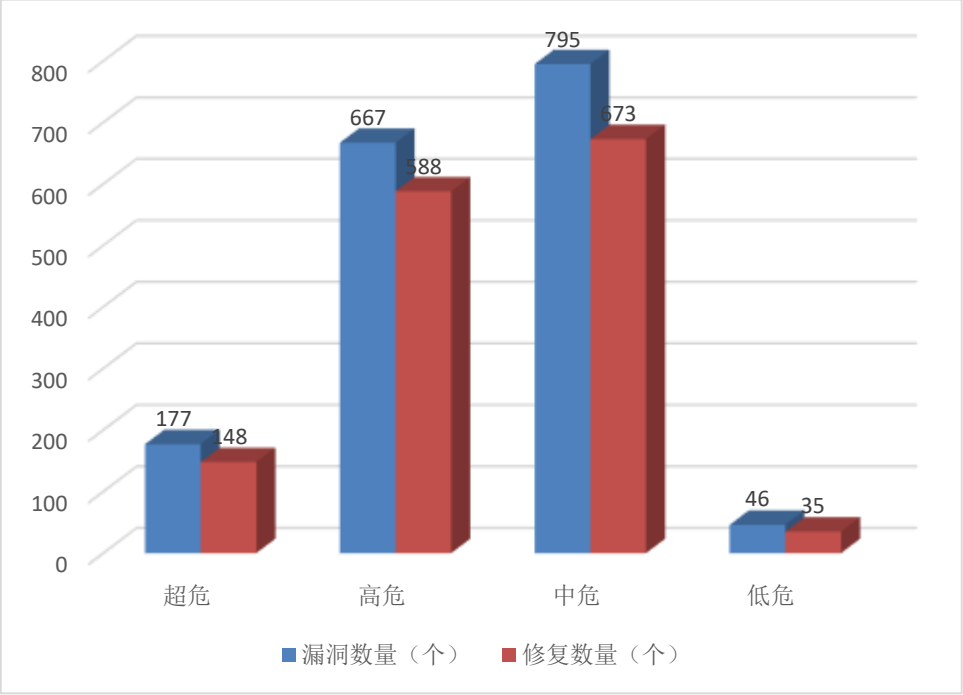

图 3　2020 年 6 月漏洞修复数量统计

1.3.2 厂商修复情况

6 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Google、Microsoft、Cisco 等十个厂商共 605 条漏洞，占本月漏洞总数的 35.91%，漏洞修复率为 98.35%，详细情况见表 4。多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中 Google、Microsoft、IBM、Foxit、Atlassian、Intel、Qualcomm 等公司本月漏洞修复率均为 100%，共 595 条漏洞已全部修复。

表 4　2020 年 6 月厂商修复情况统计表

序号	厂商名称	漏洞数量（个）	修复数量	修复率
1	Google	135	135	100.00%
2	Microsoft	130	130	100.00%
3	Cisco	89	86	96.63%
4	IBM	65	65	100.00%
5	Foxit	48	48	100.00%
6	Adobe	36	34	94.44%
7	Atlassian	32	32	100.00%
8	Intel	25	25	100.00%
9	Qualcomm	23	23	100.00%
10	Linux 基金会	22	17	77.27%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 177 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 6 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202006-031	GESTIÓNINTEGRAL ONLINE	多款 Schneider Electric 产品 SQL 注入漏洞 (CNNVD-202006-1083)
		CNNVD-202006-053	个人开发者	
		CNNVD-202006-423	rConfig	
		CNNVD-202006-425		
		CNNVD-202006-426		
		CNNVD-202006-427		
		CNNVD-202006-1024	Sokkia	
		CNNVD-202006-1083	Schneider Electric	
		CNNVD-202006-1236	gVectors 团队	
		CNNVD-202006-1551	Sourcecodester	
2	代码问题	CNNVD-202006-035	Qualcomm	IBM WebSphere Application Server 代码问题漏洞 (CNNVD-202006-494)
		CNNVD-202006-062		
		CNNVD-202006-422	Fortinet	
		CNNVD-202006-453	PostgreSQL 组织	
		CNNVD-202006-471	Foxit	
		CNNVD-202006-494	IBM	
		CNNVD-202006-516		

		CNNVD-202006-619	SAP	
		CNNVD-202006-876	个人开发者	
		CNNVD-202006-900	VMware	
		CNNVD-202006-1651		
		CNNVD-202006-908	HCL Technologies	
		CNNVD-202006-1004	Naviwebs	
		CNNVD-202006-1209	Mitsubishi Electric	
3	访问控制错误	CNNVD-202006-040	Qualcomm	Qualcomm APQ8053、Rennell 和 SDX20 访问控制错误漏洞(CNNVD-202006-040)
		CNNVD-202006-261	GE	
		CNNVD-202006-316	Aruba Networks	
		CNNVD-202006-824	Siemens	
		CNNVD-202006-1538	CyberArk Software	
		CNNVD-202006-1663	Mobile Industrial Robots	
4	缓冲区错误	CNNVD-202006-041	FarSite Communications	Treck TCP/IP stack 缓冲区错误漏洞(CNNVD-202006-1093)
		CNNVD-201705-889	个人开发者	
		CNNVD-201705-895		
		CNNVD-202006-1524		
		CNNVD-202006-1526		
		CNNVD-202006-1540		
		CNNVD-202006-1560		
		CNNVD-202006-028	Qualcomm	
		CNNVD-202006-030		
		CNNVD-202006-032		
		CNNVD-202006-045		
		CNNVD-202006-051		
		CNNVD-202006-077		
		CNNVD-202006-149	Google	
		CNNVD-202006-154		
		CNNVD-202006-236		
		CNNVD-202006-336	Cisco	
		CNNVD-202006-375		
		CNNVD-202006-451	Foxit	
		CNNVD-202006-474		
		CNNVD-202006-476		
		CNNVD-202006-479		
		CNNVD-202006-490	Samsung	
		CNNVD-202006-491		
		CNNVD-202006-511	MiniShare 项目	
		CNNVD-202006-560	Linux 基金会	

		CNNVD-202006-795	Intel	
		CNNVD-202006-830	Advantech	
		CNNVD-202006-884	Meetecho	
		CNNVD-202006-993	Morgan Stanley	
		CNNVD-202006-1010	TRENDnet	
		CNNVD-202006-1029	Meetecho	
		CNNVD-202006-1030		
		CNNVD-202006-1093	Treck	
		CNNVD-202006-1183	LibVNCServer 项目	
		CNNVD-202006-1186		
		CNNVD-202006-1187		
		CNNVD-202006-1210	Mitsubishi Electric	
		CNNVD-202006-1237	Sophos	
		CNNVD-202006-1276	ARM	
		CNNVD-202006-1277		
		CNNVD-202006-1279		
		CNNVD-202006-1563	FreeRDP 团队	
		CNNVD-202006-1567		
		CNNVD-202006-1571		
		CNNVD-202006-1575		
		CNNVD-202006-1581		
		CNNVD-202006-1596	DrayTek	
5	其他	CNNVD-202006-033	NEC	Foxit Reader 和 PhantomPDF 安全漏洞 (CNNVD-202006-432)
		CNNVD-202006-150	Google	
		CNNVD-202006-171		
		CNNVD-202006-310	Apache 软件基金会	
		CNNVD-202006-410	IBM	
		CNNVD-202006-831		
		CNNVD-202006-432	Foxit	
		CNNVD-202006-496	Samsung	
		CNNVD-202006-513	LG	
		CNNVD-202006-514		
		CNNVD-202006-515		
		CNNVD-202006-558	Linux 基金会	
		CNNVD-202006-570		
		CNNVD-202006-749	TIBCO Software	
		CNNVD-202006-868	HashiCorp	
		CNNVD-202006-899	Artica	
		CNNVD-202006-1020	Lansweeper	
		CNNVD-202006-1025	GOG	
		CNNVD-202006-1050	OpenText	

		CNNVD-202006-1102	Schneider Electric	
		CNNVD-202006-1112		
		CNNVD-202006-1184	LibVNCServer 项目	
		CNNVD-202006-1322	Open-iSCSI 项目	
		CNNVD-202006-1558	Unisys	
		CNNVD-202006-1572	Global RADAR	
		CNNVD-202006-1583	Adobe	
		CNNVD-202006-1586	Mitsubishi Electric	
		CNNVD-202006-1590		
		CNNVD-202006-1654	VMware	
		CNNVD-202006-1656		
		CNNVD-202006-1672	SolarWinds	
		CNNVD-202006-1662	Mobile Industrial Robots	
		CNNVD-202006-1675		
		CNNVD-202006-1714		
		CNNVD-202006-1692	Xiaomi	
		CNNVD-202006-1809	个人开发者	
		CNNVD-202006-1815		
6	授权问题	CNNVD-202006-321	GitHub	Apache Shiro 授权问题漏洞(CNNVD-202006-1047)
		CNNVD-202006-593	Huawei	
		CNNVD-202006-627	SAP	
		CNNVD-202006-1027	Light Code Labs	
		CNNVD-202006-1047	Apache 软件基金会	
		CNNVD-202006-1556		
		CNNVD-202006-1171	Cisco	
		CNNVD-202006-1797	ZyXEL	
7	输入验证错误	CNNVD-202006-057	Qualcomm	Android System 输入验证错误漏洞(CNNVD-202006-084)
		CNNVD-202006-084	Google	
		CNNVD-202006-322	个人开发者	
		CNNVD-202006-856		
		CNNVD-202006-437	Elliptic 项目	
		CNNVD-202006-555	Apache 软件基金会	
		CNNVD-202006-750	TIBCO Software	
		CNNVD-202006-854	node-extend 项目	
		CNNVD-202006-855	access-policy 项目	
		CNNVD-202006-1097	Treck	
		CNNVD-202006-1121		
		CNNVD-202006-1182	LibVNCServer 项目	
		CNNVD-202006-916	Rockwell Automation	
		CNNVD-202006-1211		
		CNNVD-202006-1224		
		CNNVD-202006-1323	CasperJS 团队	

8	信任管理问题	CNNVD-202006-283	IBM	IBM Security Guardium 信任管理问题漏洞 (CNNVD-202006-283)
		CNNVD-202006-974		
		CNNVD-202006-431	Foxit	
		CNNVD-202006-625	SAP	
		CNNVD-202006-981	GeoVision	
		CNNVD-202006-1079	Schneider Electric	
		CNNVD-202006-1665	Mobile Industrial Robots	
		CNNVD-202006-1666		
		CNNVD-202006-1667		

1. 多款 Schneider Electric 产品 SQL 注入漏洞（CNNVD-202006-1083）

Schneider Electric MTN6501-0001 – U.Motion – KNX Server 等都是法国施耐德电气（Schneider Electric）公司的产品。

多款 Schneider Electric 产品中存在 SQL 注入漏洞。攻击者可利用该漏洞执行任意代码。以下产品及版本受到影响：MTN6501-0001 – U.Motion – KNX Server；MTN6501-0002 – U.Motion – KNX Server Plus；MTN6260-0410 – U.Motion KNX server Plus, Touch 10；MTN6260-0415 – U.Motion KNX server Plus, Touch 15；MTN6260-0310 – U.Motion KNX Client Touch 10；MTN6260-0315 – U.Motion KNX Client Touch 15。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.se.com/ww/en/download/document/SEVD-2020-133-03/

2. IBM WebSphere Application Server 代码问题漏洞（CNNVD-202006-494）

IBM WebSphere Application Server（WAS）是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，

也是 IBMWebSphere 软件平台的基础。

IBM WAS 9.0 版本和 8.5 版本中存在安全漏洞。远程攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ibm.com/support/pages/security-bulletin-websphere-application-server-vulnerable-remote-code-execution-vulnerability-cve-2020-4450

3. Qualcomm APQ8053、Rennell 和 SDX20 访问控制错误漏洞（CNNVD-202006-040）

Qualcomm SDX20 等都是美国高通（Qualcomm）公司的产品。SDX20 是一款调制解调器。Qualcomm APQ8053 是一款中央处理器（CPU）产品。Rennell 是一款中央处理器（CPU）产品。

Qualcomm APQ8053、Rennell 和 SDX20 中的 On-Device Logging 存在访问控制错误漏洞。攻击者可借助特制请求利用该漏洞绕过访问限制。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.qualcomm.com/company/product-security/bulletins/june-2020-security-bulletin

4. Treck TCP/IP stack 缓冲区错误漏洞（CNNVD-202006-1093）

Treck TCP/IP 是美国 Treck 公司的一套专用于嵌入式系统的 TCP（传输控制协议）/IP（网际互连协议）套件。

Treck TCP/IP stack 5.0.1.35 之前版本中存在缓冲区错误漏洞。攻

击者可借助格式错误的 IPv6 数据包利用该漏洞执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://treck.com/vulnerability-response-information/

5. Foxit Reader 和 PhantomPDF 安全漏洞（CNNVD-202006-432）

Foxit Reader 和 Foxit PhantomPDF 都是中国福昕（Foxit）公司的一款 PDF 文档阅读器。

Foxit Reader 9.7.2 之前版本和 PhantomPDF 9.7.2 之前版本中的 CAS 服务存在安全漏洞，该漏洞源于程序没有对登陆失败的次数进行限制。攻击者可利用该漏洞进行暴力破解攻击。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.foxitsoftware.com/support/security-bulletins.php

6. Apache TomEE 授权问题漏洞（CNNVD-202006-1047）

Apache TomEE 是美国阿帕奇软件（Apache Software）基金会的一款轻量级的 Java EE 应用程序服务器。

Apache TomEE 中存在授权问题漏洞。攻击者可通过使用‘useJMX=true‘参数发送特制的请求利用该漏洞打开 JMX 端口。以下产品及版本受到影响：Apache TomEE 8.0.0-M1 版本至 8.0.1 版本，7.1.0 版本至 7.1.2 版本，7.0.0-M1 版本至 7.0.7 版本，1.0.0 版本至 1.7.5 版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/rbd23418646dedda70a546331ea1c1d115b8975b7e7dc452d10e2e773%40%3Cdev.tomee.apache.org%3E

7. Android System 输入验证错误漏洞（CNNVD-202006-084）

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。System 是其中的一个系统组件。

Android 中的 System 存在安全漏洞。攻击者可利用该漏洞执行代码。以下产品及版本受到影响：Android 8.0 版本，8.1 版本，9 版本，10 版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://source.android.com/security/bulletin/2020-06-01#2020-06-01-security-patch-level-vulnerability-details

8. IBM Security Guardium 信任管理问题漏洞（CNNVD-202006-283）

IBM Security Guardium 是美国 IBM 公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。

IBM Security Guardium 11.1 版本中存在信任管理问题漏洞，该漏洞源于程序使用硬编码凭证（例如密码或加密密钥）来进行身份验证，与外部组件进行对外通信或加密内部数据。攻击者可利用该漏洞获取信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/6218970

1.4.2 高危漏洞实例

本月高危漏洞共 667 个，其中重点漏洞实例如表 6 所示。

表 6 2020 年 6 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	操作系统命令注入	CNNVD-202006-079	QuickBox 团队	多款 NETGEAR 产品操作系统命令注入漏洞(CNNVD-202006-1253)
		CNNVD-202006-266	IBM	
		CNNVD-202006-296	CloudBees	
		CNNVD-202006-319	Cisco	
		CNNVD-202006-357		
		CNNVD-202006-358		
		CNNVD-202006-1167		
		CNNVD-202006-747	个人开发者	
		CNNVD-202006-1539		
		CNNVD-202006-864	Palo Alto Networks	
		CNNVD-202006-865		
		CNNVD-202006-1007	TRENDnet	
		CNNVD-202006-1012		
		CNNVD-202006-1253	NETGEAR	
		CNNVD-202006-1254		
		CNNVD-202006-1256		
		CNNVD-202006-1259		
		CNNVD-202006-1260		
		CNNVD-202006-1266		
		CNNVD-202006-1547	ArticaTech	
2	代码问题	CNNVD-201705-893	个人开发者	NVIDIA Windows GPU Display Driver 代码问题漏洞(CNNVD-202006-1707)
		CNNVD-202006-056		
		CNNVD-202006-912		
		CNNVD-202006-017	Atlassian	
		CNNVD-202006-034	Verizon	
		CNNVD-202006-307	Grafana 实验室	
		CNNVD-202006-308	Cisco	

		CNNVD-202006-369		
		CNNVD-202006-389	Google	
		CNNVD-202006-419	IBM	
		CNNVD-202006-590		
		CNNVD-202006-978		
		CNNVD-202006-442	Foxit	
		CNNVD-202006-445		
		CNNVD-202006-446		
		CNNVD-202006-448		
		CNNVD-202006-450		
		CNNVD-202006-457		
		CNNVD-202006-458		
		CNNVD-202006-463		
		CNNVD-202006-468		
		CNNVD-202006-473		
		CNNVD-202006-475		
		CNNVD-202006-478		
		CNNVD-202006-510	libupnp 项目	
		CNNVD-202006-637	Siemens	
		CNNVD-202006-816	Adobe	
		CNNVD-202006-820		
		CNNVD-202006-837	McAfee	
		CNNVD-202006-840		
		CNNVD-202006-881	Meetecho	
		CNNVD-202006-883		
		CNNVD-202006-897	Artica	
		CNNVD-202006-898		
		CNNVD-202006-911	Rockwell Automation	
		CNNVD-202006-1746		
		CNNVD-202006-915	Redash	
		CNNVD-202006-986	Viki Solutions	
		CNNVD-202006-991	Apache 软件基金会	
		CNNVD-202006-1040	个人开发者	
		CNNVD-202006-1043	DigDash	
		CNNVD-202006-1070	FasterXML	
		CNNVD-202006-1175	LibVNCServer 项目	
		CNNVD-202006-1180		

		CNNVD-202006-1208	Mitsubishi Electric	
		CNNVD-202006-1529	Information Builders	
		CNNVD-202006-1536	Kordil	
		CNNVD-202006-1542	Fortinet	
		CNNVD-202006-1552	Rakuten	
		CNNVD-202006-1650	VMware	
		CNNVD-202006-1707	NVIDIA	
		CNNVD-202006-1890	Atlassian	
3	缓冲区错误	CNNVD-201705-890	个人开发者	Microsoft Office 缓冲区错误漏洞 (CNNVD-202006-648)
		CNNVD-201705-891		
		CNNVD-201705-892		
		CNNVD-202006-605		
		CNNVD-202006-1028		
		CNNVD-202006-1038		
		CNNVD-202006-037	Qualcomm	
		CNNVD-202006-048		
		CNNVD-202006-145	Perl 社区	
		CNNVD-202006-086	Google	
		CNNVD-202006-153		
		CNNVD-202006-157		
		CNNVD-202006-158		
		CNNVD-202006-167		
		CNNVD-202006-183		
		CNNVD-202006-198		
		CNNVD-202006-204		
		CNNVD-202006-213		
		CNNVD-202006-218		
		CNNVD-202006-223		
		CNNVD-202006-242		
		CNNVD-202006-244		
		CNNVD-202006-394		
		CNNVD-202006-395		
		CNNVD-202006-262	ASUS	
		CNNVD-202006-270	vm-memory 项目	

		CNNVD-202006-291	Joyent	
		CNNVD-202006-378	libjpeg-turbo	
		CNNVD-202006-456	Foxit	
		CNNVD-202006-472		
		CNNVD-202006-477		
		CNNVD-202006-509	Linux 基金会	
		CNNVD-202006-556		
		CNNVD-202006-607	VideoLAN 组织	
		CNNVD-202006-634	VMware	
		CNNVD-202006-641	Siemens	
		CNNVD-202006-703	Intel	
		CNNVD-202006-762		
		CNNVD-202006-812		
		CNNVD-202005-444	Microsoft	
		CNNVD-202006-638		
		CNNVD-202006-644		
		CNNVD-202006-645		
		CNNVD-202006-648		
		CNNVD-202006-649		
		CNNVD-202006-650		
		CNNVD-202006-733		
		CNNVD-202006-738		
		CNNVD-202006-744		
		CNNVD-202006-756		
		CNNVD-202006-788		
		CNNVD-202006-804	IBM	
		CNNVD-202006-807		
		CNNVD-202006-809		
		CNNVD-202006-810		
		CNNVD-202006-1876		
		CNNVD-202006-863	Palo Alto Networks	
		CNNVD-202006-924	HashiCorp	
		CNNVD-202006-1005	TRENDnet	
		CNNVD-202006-1006		
		CNNVD-202006-1008		
		CNNVD-202006-1009		

		CNNVD-202006-1014		
		CNNVD-202006-1034	IJG	
		CNNVD-202006-1052	JerryScript 项目	
		CNNVD-202006-1062	Cypress Semiconductor	
		CNNVD-202006-1087	Schneider Electric	
		CNNVD-202006-1090	Treck	
		CNNVD-202006-1096	TP-Link	
		CNNVD-202006-826	Adobe	
		CNNVD-202006-1088		
		CNNVD-202006-1092		
		CNNVD-202006-1095		
		CNNVD-202006-828		
		CNNVD-202006-832		
		CNNVD-202006-1099		
		CNNVD-202006-1101		
		CNNVD-202006-1104		
		CNNVD-202006-1108		
		CNNVD-202006-1110		
		CNNVD-202006-1113		
		CNNVD-202006-1116		
		CNNVD-202006-1118		
		CNNVD-202006-1120		
		CNNVD-202006-1123		
		CNNVD-202006-1125		
		CNNVD-202006-1127		

		CNNVD-202006-1128		
		CNNVD-202006-1130		
		CNNVD-202006-1131		
		CNNVD-202006-1134		
		CNNVD-202006-1122	FFmpeg 团队	
		CNNVD-202006-1155	Cisco	
		CNNVD-202006-1157		
		CNNVD-202006-1158		
		CNNVD-202006-1159		
		CNNVD-202006-1160		
		CNNVD-202006-1161		
		CNNVD-202006-1162		
		CNNVD-202006-1163		
		CNNVD-202006-1164		
		CNNVD-202006-1165		
		CNNVD-202006-1168		
		CNNVD-202006-1169		
		CNNVD-202006-1176	LibVNCServer 项目	
		CNNVD-202006-1177		
		CNNVD-202006-1220	Rockwell Automation	
		CNNVD-202006-1696	DrayTek	
4	跨站请求伪造	CNNVD-202006-018	Atlassian	Schneider Electric Easergy T300 跨站请求伪造漏洞 (CNNVD-202006-1089)
		CNNVD-202006-273	Open Source Matters 团队	
		CNNVD-202006-299	CloudBees	
		CNNVD-202006-334	D-Link	

		CNNVD-202006-600	Couchbase	
		CNNVD-202006-742	embeDD	
		CNNVD-202006-902	F5	
		CNNVD-202006-1013	Gvectors	
		CNNVD-202006-1089	Schneider Electric	
		CNNVD-202006-1214	Drupal 社区	
		CNNVD-202006-1247	NETGEAR	
		CNNVD-202006-1325	Mattermost	
		CNNVD-202006-1528	Information Builders	
		CNNVD-202006-1610	VINADES	
		CNNVD-202006-054	个人开发者	
		CNNVD-202006-1669	个人开发者	
5	路径遍历	CNNVD-202006-075	VMware	helm 路径遍历漏洞(CNNVD-202006-1126)
		CNNVD-202006-416	Zoom	
		CNNVD-202006-429	ZOHO	
		CNNVD-202006-497	Samsung	
		CNNVD-202006-913	Rockwell Automation	
		CNNVD-202006-1082	Mailjet	
		CNNVD-202006-1126	Linux 基金会	
		CNNVD-202006-1275	EC-CUBE	
		CNNVD-202006-1530	ZyXEL	
		CNNVD-202006-1546	ArticaTech	
		CNNVD-202006-1709	SAS Institute	
		CNNVD-202006-1829	Cybozu	
6	命令注入	CNNVD-202006-1149	Cisco	多款 Cisco 产品命令注入漏洞(CNNVD-202006-1149)
		CNNVD-202006-1150		
		CNNVD-202006-1151		

		CNNVD-202006-1152		
		CNNVD-202006-1153		
		CNNVD-202006-1154		
		CNNVD-202006-1156		
		CNNVD-202006-1281	个人开发者	
7	输入验证错误	CNNVD-202006-021	Qualcomm	Microsoft SharePoint 输入验证错误漏洞 (CNNVD-202006-658)
		CNNVD-202006-025		
		CNNVD-202006-055		
		CNNVD-202006-081		
		CNNVD-202006-068		
		CNNVD-202006-078	OpenBSD 计划组	
		CNNVD-202006-148	Perl 社区	
		CNNVD-202006-155	Google	
		CNNVD-202006-175		
		CNNVD-202006-179		
		CNNVD-202006-192		
		CNNVD-202006-195		
		CNNVD-202006-237		
		CNNVD-202006-241		
		CNNVD-202006-318	Aruba Networks	
		CNNVD-202006-325	Compound Labs	
		CNNVD-202006-312	Cisco	
		CNNVD-202006-315		
		CNNVD-202006-333		
		CNNVD-202006-343		
		CNNVD-202006-344		
		CNNVD-202006-354		
		CNNVD-202006-362		
		CNNVD-202006-363		
		CNNVD-202006-367		
		CNNVD-202006-368		
		CNNVD-202006-370		
		CNNVD-202006-392		
		CNNVD-202006-1170		
		CNNVD-202006-428	NTP	
		CNNVD-202006-505	Abstrium	
		CNNVD-202006-557	Linux 基金会	

		CNNVD-202006-740		
		CNNVD-202006-563	Cheetah	
		CNNVD-202006-658	Microsoft	
		CNNVD-202006-660		
		CNNVD-202006-690		
		CNNVD-202006-695		
		CNNVD-202006-736		
		CNNVD-202006-715	Intel	
		CNNVD-202006-722		
		CNNVD-202006-727		
		CNNVD-202006-734		
		CNNVD-202006-813		
		CNNVD-202006-853	mosc 项目	
		CNNVD-202006-918	Rockwell Automation	
		CNNVD-202006-923	HashiCorp	
		CNNVD-202006-1037	Redis Labs	
		CNNVD-202006-1084	Treck	
		CNNVD-202006-1280	ARM	
		CNNVD-202006-1332	Mattermost	
		CNNVD-202006-1346		
		CNNVD-202006-1388		
		CNNVD-202006-1522	Bitdefender	
		CNNVD-202006-1855	COMMAX	
8	资源管理错误	CNNVD-202006-044	个人开发者	Mozilla Firefox 和 Firefox ESR 资源管理错误漏洞 (CNNVD-202006-252)
		CNNVD-202006-500		
		CNNVD-202006-512		
		CNNVD-202006-575		
		CNNVD-202006-058	Apple	
		CNNVD-202006-059	Qualcomm	
		CNNVD-202006-069		
		CNNVD-202006-080		
		CNNVD-202006-347	Cisco	
		CNNVD-202006-252	Mozilla 基金会	
		CNNVD-202006-152	Google	
		CNNVD-202006-399		
		CNNVD-202006-1058		
		CNNVD-202006-1582		
		CNNVD-202006-433	Foxit	
		CNNVD-202006-435		

		CNNVD-202006-436		
		CNNVD-202006-443		
		CNNVD-202006-444		
		CNNVD-202006-447		
		CNNVD-202006-449		
		CNNVD-202006-461		
		CNNVD-202006-465		
		CNNVD-202006-467		
		CNNVD-202006-827	Mitsubishi Electric	
		CNNVD-202006-886	Red Hat	
		CNNVD-202006-887	Linux 基金会	
		CNNVD-202006-998	Open-Xchange	
		CNNVD-202006-1033	IJG	
		CNNVD-202006-1100	Schneider Electric	
		CNNVD-202006-1103	Treck	
		CNNVD-202006-1232	Python 软件基金会	
		CNNVD-202006-1328	Mattermost	
		CNNVD-202006-1396		
		CNNVD-202006-1499	GitLab	
		CNNVD-202006-1578	FreeRDP 团队	

1. 多款 NETGEAR 产品操作系统命令注入漏洞

（CNNVD-202006-1253）

NETGEAR RBK752 等都是美国网件（NETGEAR）公司的一套家庭 WiFi 系统。

多款 NETGEAR 产品中存在操作系统命令注入漏洞。攻击者可通过发送特制请求利用该漏洞在系统上执行任意 Shell 命令。以下产品及版本受到影响：NETGEAR RBK752 3.2.15.25 之前版本；RBK753 3.2.15.25 之前版本；RBK753S 3.2.15.25 之前版本；RBR750 3.2.15.25 之前版本；RBS750 3.2.15.25 之前版本；RBK842 3.2.15.25 之

前版本；RBR840 3.2.15.25 之前版本；RBS840 3.2.15.25 之前版本；RBK852 3.2.15.25 之前版本；RBK853 3.2.15.25 之前版本；RBR850 3.2.15.25 之前版本；RBS850 3.2.15.25 之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054

2. NVIDIA Windows GPU Display Driver 代码问题漏洞（CNNVD-202006-1707）

NVIDIA Windows GPU Display Driver 是美国英伟达（NVIDIA）公司的一款专用于 Windows 平台的图形处理器（GPU）显卡驱动程序。

NVIDIA Windows GPU Display Driver（所有版本）中的 Direct X 11 nvwgf2um/x.dll 文件存在代码问题漏洞。攻击者可利用该漏洞导致拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://nvidia.custhelp.com/app/answers/detail/a_id/5031

3. Microsoft Office 缓冲区错误漏洞（CNNVD-202006-648）

Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。

Microsoft Office 中存在远程执行代码漏洞，该漏洞源于程序未正确处理内存中的对象。攻击者可借助特制文件利用该漏洞在当前用

户的安全上下文中执行操作。以下产品及版本受到影响：Microsoft 365 Apps for Enterprise；Microsoft Office 2016 for Mac；Microsoft Office 2019；Microsoft Office 2019 for Mac。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1321

4. Schneider Electric Easergy T300 跨站请求伪造漏洞（CNNVD-202006-1089）

Schneider Electric Easergy T300 是法国施耐德电气（Schneider Electric）公司的一款用于电力行业的远程终端单元。

使用 1.5.2 及之前版本固件的 Schneider Electric Easergy T300 中存在跨站请求伪造漏洞。攻击者可利用该漏洞以合法用户的身份执行恶意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.se.com/ww/en/download/document/SEVD-2020-161-04/

5. helm 路径遍历漏洞（CNNVD-202006-1126）

helm 是一款 Kubernetes 包管理器。

helm 3.0.0 及之后版本（3.2.4 版本已修复）中存在路径遍历漏洞。攻击者可通过发送在‘path’参数中包含‘/../’序列的 tar 文件利用该漏洞覆盖系统上的任意文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/helm/helm/releases/tag/v3.2.4

6. 多款 Cisco 产品命令注入漏洞（CNNVD-202006-1149）

Cisco Small Business RV016 Multi-WAN VPN 等都是美国思科（Cisco）公司的一款 VPN 路由器。

多款 Cisco 产品中的 Web 管理界面存在命令注入漏洞，该漏洞源于程序没有正确验证用户提交的输入。远程攻击者可通过发送恶意的请求利用该漏洞以 root 权限执行任意命令。以下产品及版本受到影响：Cisco Small Business RV016 Multi-WAN VPN 4.2.3.10 及之前版本；RV042 Dual WAN VPN 4.2.3.10 及之前版本；RV042G Dual Gigabit WAN VPN 4.2.3.10 及之前版本；RV082 Dual WAN VPN 4.2.3.10 及之前版本；RV320 Dual Gigabit WAN VPN 1.5.1.05 及之前版本；RV325 Dual Gigabit WAN VPN 1.5.1.05 及之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-routers-Rj5JRfF8

7. Microsoft SharePoint 输入验证错误漏洞（CNNVD-202006-658）

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。

Microsoft SharePoint 中存在远程代码执行漏洞，该漏洞源于程序未正确识别和过滤不安全的 ASP.NET Web 控件。攻击者可借助特制的页面利用该漏洞在 SharePoint 应用程序池进程的安全上下文中执行

操作。以下产品及版本受到影响：Microsoft SharePoint Enterprise Server 2016，Microsoft SharePoint Foundation 2010 SP2，Microsoft SharePoint Foundation 2013 SP1，Microsoft SharePoint Server 2019。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1181

8. Mozilla Firefox 和 Firefox ESR 资源管理错误漏洞（CNNVD-202006-252）

Mozilla Firefox 和 Mozilla Firefox ESR 都是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。

Mozilla Firefox 77 之前版本和 Firefox ESR 68.9 之前版本中 SharedWorkerService 存在资源管理错误漏洞。攻击者可利用该漏洞造成浏览器崩溃。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2020-20/

https://www.mozilla.org/en-US/security/advisories/mfsa2020-21/

二、接报漏洞情况

本月接报漏洞 7943 个，其中信息技术产品漏洞（通用型漏洞）177 个，网络信息系统漏洞（事件型漏洞）7766 个。

表 7 2020 年 6 月漏洞接报情况

序号	报送单位	漏洞总量

1	网神信息技术（北京）股份有限公司	4060
2	上海斗象信息科技有限公司	2732
3	长春嘉诚信息技术股份有限公司	182
4	内蒙古奥创科技有限公司	178
5	北京山石网科信息技术有限公司	171
6	听潮盛世信息技术有限公司	105
7	北京华云安信息技术有限公司	45
8	四叶草信息安全有限公司	40
9	北京数字观星科技有限公司	37
10	太极计算机股份有限公司	34
11	安徽华云网安信息技术有限公司	30
12	北京赋云安运营科技有限公司	30
13	北京神州绿盟科技有限公司	28
14	绿盟科技集团股份有限公司	27
15	北京天融信网络安全技术有限公司	25
16	山东新潮信息技术有限公司	21
17	杭州默安科技有限公司	20
18	广州锦行网络科技有限公司	20
19	星云博创科技有限公司漏洞	19
20	中兴通讯	15
21	远江盛邦(北京)网络安全科技股份有限公司	10
22	北京云测信息技术有限公司	10
23	西安交大捷普科技有限公司	9

24	南京东科优信网络安全技术研究院有限公司	8
25	中国电信集团系统集成有限责任公司	7
26	安全邦（北京）信息技术有限公司	6
27	北京启明星辰信息安全技术有限公司	6
28	上海安识网络科技有限公司	6
29	深信服电子科技有限公司	6
30	个人	6
31	北京圣博润高新技术股份有限公司	5
32	北京天地和兴科技有限公司	5
33	安徽锋刃信息科技有限公司	4
34	东软集团股份有限公司	4
35	北京智游网安科技有限公司	4
36	北京梆梆安全科技有限公司	3
37	腾讯安全玄武实验室	3
38	北京知道创宇信息技术股份有限公司	2
39	北京奇虎科技有限公司	2
40	北京江南天安科技有限公司	2
41	南京中新赛克科技有限责任公司	2
42	浙江宇视科技有限公司	2
43	北京中测安华科技有限公司	1
44	山西轩辕信息安全技术有限公司	1
45	长亭科技	1
46	安徽长泰信息安全服务有限公司	1

47	北京威努特技术有限公司	1
48	哈尔滨安天科技集团股份有限公司	1
49	恒安嘉新（北京）科技股份公司	1
50	美国印第安纳大学伯明顿分校，中国科学院信息工程研究所	1
51	锐捷网络股份有限公司	1
52	天津市兴先道科技有限公司	1
53	掌控安全	1
54	中兴网信	1
报送总计		7943

三、重大漏洞预警

3.1 微软多个安全漏洞的预警

近日，微软官方发布了多个安全漏洞的公告，Microsoft ChakraCore 和 Edge 安全漏洞（CNNVD-202006-638、CVE-2020-1073）、Microsoft Windows Graphics Device Interface 安全漏洞（CNNVD-202006-733、CVE-2020-1248）、Microsoft Windows OLE 安全漏洞（CNNVD-202006-695、CVE-2020-1281）等多个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

2020 年 6 月 9 日，微软发布了 2020 年 6 月份安全更新，共 129 个漏洞的补丁程序，CNNVD 对这些漏洞进行了收录。本次更新涵盖了 Windows 操作系统、Windows 应用商店、IE/Edge 浏览器、ChakraCore、Visual Studio、Office、等多个 Windows 平台下应用软件和组件。微软多个产品和系统版本受漏洞影响，具体影响范围可访问 https://portal.msrc.microsoft.com/zh-cn/security-guidance 查询，其中部分重要漏洞详情如下：

1、Microsoft ChakraCore 和 Edge 安全漏洞（CNNVD-202006-638、CVE-2020-1073）

漏洞简介：ChakraCore 脚本引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者便可控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

2、Microsoft Windows Graphics Device Interface 安全漏洞（CNNVD-202006-733、CVE-2020-1248）

Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有

完全用户权限的新帐户。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统权限的用户受到的影响更小。

3、Microsoft Windows OLE 安全漏洞（CNNVD-202006-695、CVE-2020-1281）

漏洞简介： 当 Microsoft Windows OLE 无法正确验证用户输入时，会触发远程代码执行漏洞。攻击者可以利用此漏洞以执行恶意代码。要利用此漏洞，攻击者必须诱使用户在网页或电子邮件中打开经特殊设计的文件或程序。

4、Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202006-683、CVE-2020-1299）

漏洞简介：Windows 系统如果处理了.LNK 文件，则会触发一个远程代码执行漏洞。成功利用此漏洞的攻击者可能会获得与本地用户相同的用户权限。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。

5、Microsoft SharePoint 安全漏洞（CNNVD-202006-658、CVE-2020-1181）

漏洞简介：当 Microsoft SharePoint Server 无法正确识别和筛选不安全的 ASP.NET Web 控件时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经特殊设计的页面在 SharePoint 应用程序池进程中执行操作。若要利用此漏洞，经过身份验证的用户必须在受影响的 Microsoft SharePoint Server 版本上创建并调用经特殊设计的页面。

6、Microsoft Internet Explorer、Edge 和 ChakraCore 安全漏洞(CNNVD-202006-644、CVE-2020-1219)

漏洞简介：Microsoft 浏览器访问内存中对象的方式中存在远程代码执行漏洞。此漏洞可能以一种允许攻击者在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，那么攻击者便可控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

7、Microsoft Windows Shell 安全漏洞(CNNVD-202006-690、CVE-2020-1286)

漏洞简介：当 Windows Shell 不正确地验证文件路径时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户以管理员身份登录，则攻击者可以控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有提升特权的新帐户。与拥有管理权限的用户相比，帐户被配置为拥有较少系统权限的用户受到的影响更小。

8、Microsoft Windows 和 Windows Server 安全漏洞(CNNVD-202006-682、CVE-2020-1300)

漏洞简介：当 Microsoft Windows 无法正确处理 cabinet 文件时，会触发远程代码执行漏洞。若要利用此漏洞，攻击者需要诱使用户打开经特殊设计的 cabinet 文件或欺骗网络打印机并诱骗用户安装伪装成打印机驱动程序的恶意 cabinet 文件。

9、Microsoft Internet Explorer VBScript Engine 安全漏洞(CNNVD-202006-645、CVE-2020-1213)(CNNVD-202006-646、CVE-2020-1216)

漏洞简介：VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。该漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者便可控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。

10、Microsoft Excel 安全漏洞 (CNNVD-202006-650、CVE-2020-1226)(CNNVD-202006-649、CVE-2020-1225)

漏洞简介：当 Microsoft Excel 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，那么攻击者就可以控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。

11、Microsoft Office 安全漏洞(CNNVD-202006-648、CVE-2020-1321)

漏洞简介：当 Microsoft Office 软件无法正确处理内存中的对象时，会触发远程代码执行漏洞。成功利用此漏洞的攻击者可以使用经

特殊设计的文件在当前用户的上下文中执行操作。例如，文件可以代表登录用户使用与当前用户相同的权限执行操作。

12、Microsoft Windows Server Message Block 安全漏洞（CNNVD-202006-681、CVE-2020-1301）

漏洞简介：该漏洞是由于 SMB 协议在处理某些请求时，进入了错误流程，导致攻击者可以触发远程代码执行漏洞。成功利用此漏洞的攻击者可以在目标系统上执行恶意代码。若要利用此漏洞，经身份验证的攻击者需要向目标服务器发送经特殊设计的数据包。

修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，尽快采取修补措施。微软官方链接地址如下：

序号	漏洞名称	官方链接
1	Microsoft ChakraCore 和 Edge 安全漏洞（CNNVD-202006-638、CVE-2020-1073）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1073
2	Microsoft Windows Graphics Device Interface 安全漏洞（CNNVD-202006-733、CVE-2020-1248）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1248
3	Microsoft Windows OLE 安全漏洞（CNNVD-202006-695、CVE-2020-1281）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1281
4	Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202006-683、CVE-2020-1299）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1299
5	Microsoft SharePoint 安全漏洞（CNNVD-202006-658、CVE-2020-1181）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1181
6	Microsoft Internet Explorer、Edge 和 ChakraCore 安全漏洞(CNNVD-202006-644、CVE-2020-1219)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1219
7	Microsoft Windows Shell 安全漏洞(CNNVD-202006-690、CVE-2020-1286)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1286
8	Microsoft Windows 和 Windows Server 安全漏洞(CNNVD-202006-682、CVE-2020-1300)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1300
9	Microsoft Internet Explorer VBScript Engine	https://portal.msrc.microsoft.com/zh-CN/security-guidance/ad

	安全漏洞(CNNVD-202006-645、CVE-2020-1213)(CNNVD-202006-646、CVE-2020-1216)	visory/CVE-2020-1213 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1216
10	Microsoft Excel 安全漏洞(CNNVD-202006-650、CVE-2020-1226)(CNNVD-202006-649、CVE-2020-1225)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1226 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1225
11	Microsoft Office 安全漏洞(CNNVD-202006-648、CVE-2020-1321)	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1321
12	Microsoft Windows Server Message Block 安全漏洞（CNNVD-202006-681、CVE-2020-1301）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1301

3.2 IBM WebSphere Application Server 远程代码执行漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 IBM WebSphere Application Server 远程代码执行漏洞(CNNVD-202006-494、 CVE-2020-4450))情况的报送。攻击者可利用漏洞在未授权的情况下发送攻击数据,实现远程代码执行，最终控制 IBM WebSphere 服务器。IBM WebSphere Application Server Version9.0.0.0-9.0.5.4、8.5.0.0-8.5.5.17、8.0.0.0-8.0.0.15、7.0.0.0-7.0.0.45 等多个版本均受漏洞影响。目前，IBM 官方已经发布补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

漏洞简介

IBM WebSphere Application Server（WAS）是美国 IBM 公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。该漏洞是由于 IIOP 协议上的

反序列化造成，未经身份认证的攻击者可以通过 IIOP 协议远程攻击 IBM WebSphere 服务器，在目标服务端执行任意代码，获取系统权限，进而完全控制服务器。

危害影响

成功利用该漏洞的攻击者可以对目标系统实现远程代码执行，获取系统权限，进而完全控制服务器。IBM WebSphere Application Server Version9.0.0.0-9.0.5.4 、 8.5.0.0-8.5.5.17 、 8.0.0.0-8.0.0.15、7.0.0.0-7.0.0.45 等多个版本均受漏洞影响。

修复建议

目前，IBM 官方已经发布补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。IBM 官方更新链接如下：

下载地址：https://www.ibm.com/support/pages/node/6220276