北京师范大学网络信息安全通告

2020 年 4 月报告

北京师范大学信息网络中心

2020年 5 月

目录

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 4 月份新增安全漏洞共 2155 个，从厂商分布来看，NETGEAR 公司产品的漏洞数量最多，共发布 463 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 16.10%。本月新增漏洞中，超危漏洞 277 个、高危漏洞 873 个、中危漏洞 945 个、低危漏洞 60 个，相应修复率分别为 77.62%、89.23%、87.83%以及 85.00%。合计 1875 个漏洞已有修复补丁发布，本月整体修复率 87.01%。

截至 2020 年 04 月 30 日，CNNVD 采集漏洞总量已达 144270 个。

1.1 漏洞增长概况

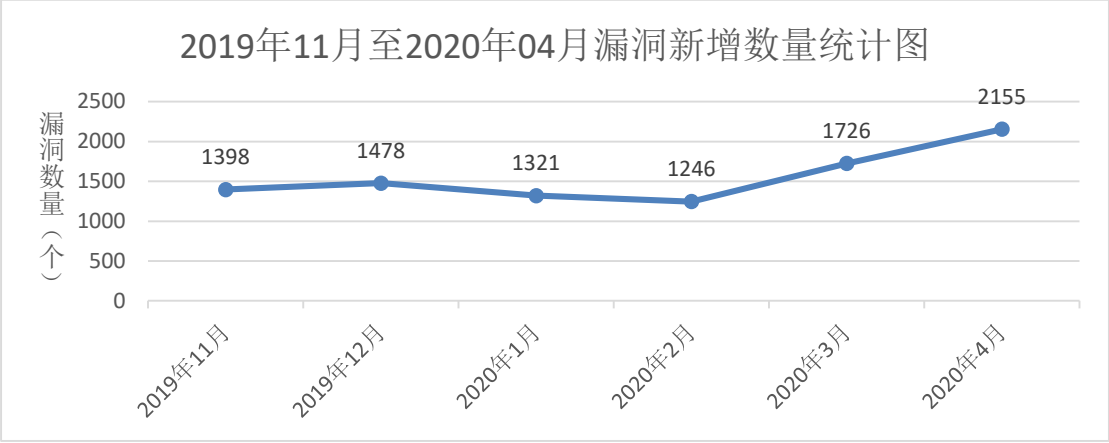

图 1 2019 年 9 月至 2020 年 4 月漏洞新增数量统计图

2020 年 4 月新增安全漏洞 2155 个，与上月（1726 个）相比增加了 24.86%。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 1554 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

4 月厂商漏洞数量分布情况如表 1 所示，NETGEAR 公司漏洞达到 463 个，占本月漏洞总量的 21.48%。

表 1　2020 年 4 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	NETGEAR	463	21.48%
2	Oracle	229	10.63%
3	Samsung	149	6.91%
4	Microsoft	113	5.24%
5	IBM	51	2.37%
6	Google	50	2.32%
7	Qualcomm	48	2.23%
8	Adobe	41	1.90%
9	F5	30	1.39%
10	SAP	29	1.35%

1.2.2 漏洞产品分布

4 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 10 漏洞数量最多，共 66 个，占主流操作系统漏洞总量的 14.25%，排名第一。

表 2　2020 年 4 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	Windows 10	66
2	Windows Server 2019	63
3	Windows Server 2016	51

4	Windows 8.1	38
5	Windows Server 2012	37
6	Windows Rt 8.1	37
7	Windows Server 2012 R2	36
8	Windows 7	36
9	Windows Server 2008	35
10	Windows Server 2008 R2	35
11	Android	15
12	Linux Kernel	14

*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

4 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 16.10%。

表 3 2020 年 4 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	缓冲区错误	347	16.10%
2	跨站脚本	227	10.53%
3	信息泄露	177	8.21%
4	输入验证错误	164	7.61%
5	注入	97	4.50%
6	代码问题	86	3.99%
7	授权问题	66	3.06%
8	资源管理错误	60	2.78%
9	操作系统命令注入	53	2.46%
10	跨站请求伪造	35	1.62%
11	路径遍历	31	1.44%
12	SQL 注入	24	1.11%
13	访问控制错误	24	1.11%
14	信任管理问题	23	1.07%
15	权限许可和访问控制问题	14	0.65%
16	加密问题	13	0.60%

17	竞争条件问题	10	0.46%
18	数据伪造问题	8	0.37%
19	日志信息泄露	7	0.32%
20	后置链接	6	0.28%
21	命令注入	6	0.28%
22	代码注入	5	0.23%
23	安全特征问题	3	0.14%
24	环境问题	2	0.09%
25	数字错误	2	0.09%
26	格式化字符串错误	1	0.05%
27	其他	664	30.81%

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。4 月漏洞危害等级分布如图 2 所示，其中超危漏洞 277 条，占本月漏洞总数的 12.85%。

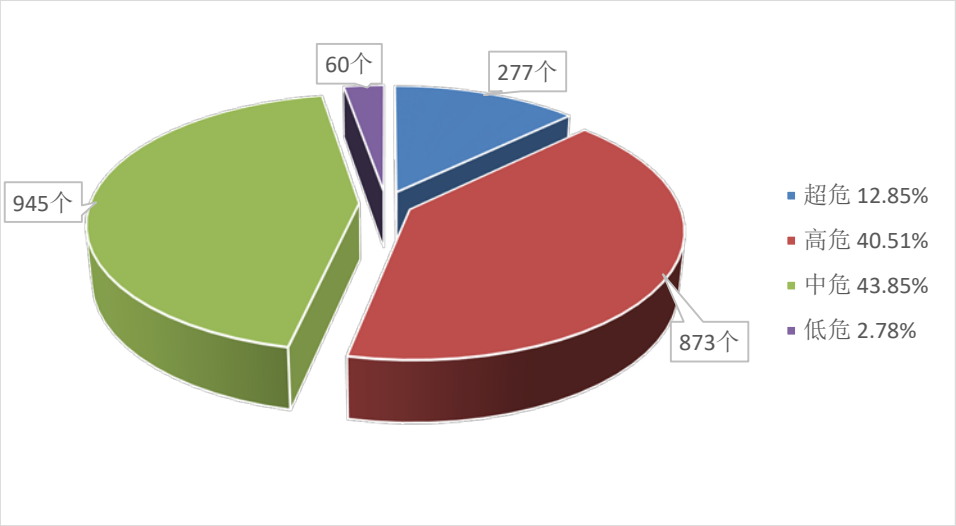

图 2　2020 年 4 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

4 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 89.23%，超危漏洞修复率最低，比例为 77.62%。总体来看，本月整体修复率，由上月的 75.78%上升至本月的 87.01%。

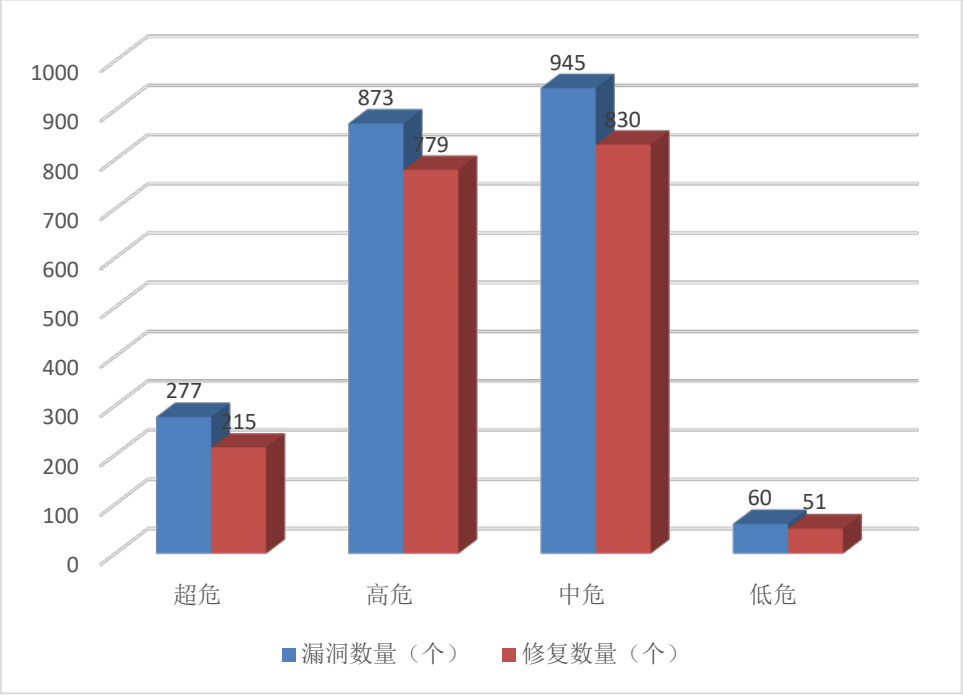

图 3　2020 年 4 月漏洞修复数量统计

1.3.2 厂商修复情况

4 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 NETGEAR、Oracle、Samsung 等十个厂商共 1203 条漏洞，占本月漏洞总数的 55.82%，漏洞修复率为 98.59%，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 NETGEAR、Oracle、Microsoft、Google、Qualcomm、Adobe、SAP 等公司本月漏洞修复率均为 100%，共 1186 条漏洞已全部修复。

表 4　2020 年 4 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	NETGEAR	463	463	100.00%
2	Oracle	229	229	100.00%
3	Samsung	149	148	99.33%
4	Microsoft	113	113	100.00%
5	IBM	51	50	98.04%
6	Google	50	50	100.00%
7	Qualcomm	48	48	100.00%
8	Adobe	41	41	100.00%
9	F5	30	15	50.00%
10	SAP	29	29	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 277 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 4 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	注入	CNNVD-202004-011	Apache 软件基金会	多款 NETGEAR 产品注入漏洞
		CNNVD-202004-019	Aruba Networks	
		CNNVD-202004-297	CIPPlanner	
		CNNVD-202004-451	cpp-httplib 项目	
		CNNVD-202004-1158	NETGEAR	
		CNNVD-202004-1950		
2	信任管理问题	CNNVD-202004-390	OpsRamp	Apache IoTDB 信任管理问题漏洞
		CNNVD-202004-507	Juniper Networks	
		CNNVD-202004-508		
		CNNVD-202004-1448	8x8	
		CNNVD-202004-2028	NETGEAR	
		CNNVD-202004-2195	Apache 软件基金会	
3	输入验证错误	CNNVD-202004-205	Qualcomm	Apple iOS、macOS Mojave 和 tvOS 802.1X 组件输入验证错误漏洞
		CNNVD-202004-2168	TestLink 团队	
		CNNVD-202004-1934	Teeworlds 团队	
		CNNVD-202004-1979	Squid	
		CNNVD-202004-927	Siemens	
		CNNVD-202004-662	SAP	
		CNNVD-202004-293	Samsung	

		CNNVD-202004-339		
		CNNVD-202004-343		
		CNNVD-202004-414		
		CNNVD-202004-456		
		CNNVD-202004-457		
		CNNVD-202004-206	Qualcomm	
		CNNVD-202004-208		
		CNNVD-202004-1976	Ntop	
		CNNVD-202004-1157	NETGEAR	
		CNNVD-202004-1207		
		CNNVD-202004-1435	Mitel Networks	
		CNNVD-202004-2190	libgit2	
		CNNVD-202004-2191		
		CNNVD-202004-1430	LG	
		CNNVD-202004-1431		
		CNNVD-202004-1099	Cisco	
		CNNVD-202004-1109		
		CNNVD-202004-1970	Blue Link Labs 实验室	
		CNNVD-202004-1334	Aviatrix Systems	
		CNNVD-202004-1185	Ascensio System	
		CNNVD-202004-1187		
		CNNVD-202004-1447	Apple	
4	授权问题	CNNVD-202004-179	CIPPlanner	Fortinet FortiMail 和 FortiVoice Entreprise 授权问题漏洞
		CNNVD-202004-437	Samsung	
		CNNVD-202004-622	total-soft	
		CNNVD-202004-1183	DAViCal 项目	
		CNNVD-202004-1436	LG	
		CNNVD-202004-1949	JetBrains	
		CNNVD-202004-1957	Huawei	
		CNNVD-202004-2193	Fortinet	
5	其他	CNNVD-202004-031	Avast	Oracle Fusion Middleware 安全漏洞
		CNNVD-202004-139	ZOHO	
		CNNVD-202004-945	Triangle MicroWorks	
		CNNVD-202004-1337	Schneider Electric	
		CNNVD-202004-681	SAP	
		CNNVD-202004-245	Samsung	
		CNNVD-202004-270		
		CNNVD-202004-442		
		CNNVD-202004-465		
		CNNVD-202004-477		

		CNNVD-202004-518	
		CNNVD-202004-2446	SaltStack
		CNNVD-202004-2448	
		CNNVD-202004-358	Rank Math
		CNNVD-202004-273	Qualcomm
		CNNVD-202004-810	Oracle
		CNNVD-202004-811	
		CNNVD-202004-812	
		CNNVD-202004-814	
		CNNVD-202004-821	
		CNNVD-202004-971	
		CNNVD-202004-989	
		CNNVD-202004-992	
		CNNVD-202004-996	
		CNNVD-202004-1017	
		CNNVD-202004-1239	NETGEAR
		CNNVD-202004-2022	
		CNNVD-202004-2032	
		CNNVD-202004-280	Mozilla 基金会
		CNNVD-202004-891	Microsoft
		CNNVD-202004-1426	LG
		CNNVD-202004-1429	
		CNNVD-202004-1931	JetBrains
		CNNVD-202004-188	HPE
		CNNVD-202004-2135	
		CNNVD-202004-2492	
		CNNVD-202004-349	HCL Technologies
		CNNVD-202004-2460	F5
		CNNVD-202004-1124	Broadcom
		CNNVD-202004-1186	Ascensio System
		CNNVD-202004-2324	Adobe
		CNNVD-202004-2325	
		CNNVD-202004-2327	
		CNNVD-202004-2329	
		CNNVD-202004-2330	
		CNNVD-202004-2353	
		CNNVD-202004-2356	
6	缓冲区错误	CNNVD-202004-199	Google	多款 Samsung 产品缓冲区错误漏洞
		CNNVD-202004-2157	Artifex Software	
		CNNVD-202004-553	Dahua	
		CNNVD-202004-2237	FFmpeg 团队	
		CNNVD-202004-203	Google	

		CNNVD-202004-209		
		CNNVD-202004-212		
		CNNVD-202004-1840	IBM	
		CNNVD-202004-1433	LG	
		CNNVD-202004-1439		
		CNNVD-202004-307	Mozilla 基金会	
		CNNVD-202004-354		
		CNNVD-202004-1283	NETGEAR	
		CNNVD-202004-2024		
		CNNVD-202004-2025		
		CNNVD-202004-2187		
		CNNVD-202004-2201		
		CNNVD-202004-377	Netty 社区	
		CNNVD-202004-202	Qualcomm	
		CNNVD-202004-204		
		CNNVD-202004-210		
		CNNVD-202004-211		
		CNNVD-202004-213		
		CNNVD-202004-216		
		CNNVD-202004-221		
		CNNVD-202004-225		
		CNNVD-202004-226		
		CNNVD-202004-230		
		CNNVD-202004-235		
		CNNVD-202004-242		
		CNNVD-202004-243		
		CNNVD-202004-253		
		CNNVD-202004-317		
		CNNVD-202004-1261		
		CNNVD-202004-1262		
		CNNVD-202004-1417		
		CNNVD-202004-244	Samsung	
		CNNVD-202004-256		
		CNNVD-202004-262		
		CNNVD-202004-266		
		CNNVD-202004-269		
		CNNVD-202004-279		
		CNNVD-202004-282		
		CNNVD-202004-304		
		CNNVD-202004-308		
		CNNVD-202004-309		
		CNNVD-202004-335		

		CNNVD-202004-348		
		CNNVD-202004-352		
		CNNVD-202004-408		
		CNNVD-202004-420		
		CNNVD-202004-421		
		CNNVD-202004-428		
		CNNVD-202004-429		
		CNNVD-202004-432		
		CNNVD-202004-444		
		CNNVD-202004-449		
		CNNVD-202004-450		
		CNNVD-202004-454		
		CNNVD-202004-461		
		CNNVD-202004-467		
		CNNVD-202004-468		
		CNNVD-202004-476		
		CNNVD-202004-593		
		CNNVD-202004-594		
		CNNVD-202004-956	Triangle MicroWorks	
7	代码问题	CNNVD-202004-090	STARFACE	Apache Heron 代码问题漏洞
		CNNVD-202004-182	CIPPlanner	
		CNNVD-202004-385	FasterXML	
		CNNVD-202004-387		
		CNNVD-202004-402	PrimeKey Solutions	
		CNNVD-202004-403	Advantech	
		CNNVD-202004-493	GitLab	
		CNNVD-202004-1195	ALLE INFORMATION	
		CNNVD-202004-1325	Apache 软件基金会	
		CNNVD-202004-1408	Veeam	
		CNNVD-202004-1410		
		CNNVD-202004-1788	Micro Star	
		CNNVD-202004-1943	Elementor 团队	
8	SQL 注入	CNNVD-202004-053	LearnDash	多款 NETGEAR 产品 SQL 注入漏洞
		CNNVD-202004-122	TestLink 团队	
		CNNVD-202004-124		
		CNNVD-202004-178	CIPPlanner	
		CNNVD-202004-1184	Ascensio System	
		CNNVD-202004-1197	ALLE INFORMATION	
		CNNVD-202004-1341	NETGEAR	
		CNNVD-202004-2160	Sophos	

1. 多款 NETGEAR 产品注入漏洞（CNNVD-202004-1158）

NETGEAR R6400 等都是美国网件（NETGEAR）公司的一款无线路由器。

多款 NETGEAR 产品中存在注入漏洞。该漏洞源于用户输入构造命令、数据结构或记录的操作过程中，网络系统或产品缺乏对用户输入数据的正确验证，未过滤或未正确过滤掉其中的特殊元素，导致系统或产品产生解析或解释方式错误。以下产品及版本受到影响：NETGEAR R6400v2 1.0.4.84 之前版本；R6700 1.0.2.8 之前版本；R6700v3 1.0.4.84 之前版本；R6900 1.0.2.8 之前版本；R7900 1.0.3.10 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/000061741/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-Routers-PSV-2019-0051

2. Apache IoTDB 信任管理问题漏洞（CNNVD-202004-2195）

Apache IoTDB 是美国阿帕奇软件（Apache Software）基金会的一款为时间序列数据设计的集成数据管理引擎，它能够提供数据收集、存储和分析服务等。

Apache IoTDB 0.9.0 版本至 0.9.1 版本和 0.8.0 版本至 0.8.2 版本中存在安全漏洞，该漏洞源于启动 IoTDB 时，31999 JMX 端口未经认证便可被访问。攻击者可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://lists.apache.org/thread.html/r3d2ff899ead64d2952fdc1fbb1f5

20ca42011ed2b4c7f786e921f6b9%40%3Cdev.iotdb.apache.org%3E

3. Apple iOS、macOS Mojave 和 tvOS 802.1X 组件输入验证错误漏洞（CNNVD-202004-1447）

Apple iOS 等都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。

Apple iOS 12.2 之前版本、macOS Mojave 10.14.4 之前版本和 tvOS 12.2 之前版本中的 802.1X 组件存在安全漏洞。攻击者可利用该漏洞拦截网络流量。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/zh-cn/HT209600

https://support.apple.com/zh-cn/HT209601

https://support.apple.com/zh-cn/HT209599

4. Fortinet FortiMail 和 FortiVoice Entreprise 授权问题漏洞（CNNVD-202004-2193）

Fortinet FortiMail 和 FortiVoice Entreprise 都是美国飞塔（Fortinet）公司的产品。FortiMail 是一套电子邮件安全网关产品。该产品提供电子邮件安全防护和数据保护等功能。FortiVoice Entreprise 是一套企业统一通信解决方案。

Fortinet FortiMail 和 FortiVoice Entreprise 中存在安全漏洞，该漏洞源于程序没有正确验证身份。远程攻击者可借助用户界面发送请求

利用该漏洞更改密码，以合法用户身份访问系统。以下产品及版本受到影响：Fortinet FortiMail 5.4.10 及之前版本，FortiMail 6.0.7 及之前版本，FortiMail 6.2.2 及之前版本；FortiVoice Entreprise 5.3 之后版本（6.0.2 版本已修复）。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://fortiguard.com/psirt/FG-IR-20-045

5. Oracle Fusion Middleware 安全漏洞（CNNVD-202004-810）

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Business Intelligence Enterprise Edition 是其中的一个为企业提供同类可视化分析和自助式发现平台的组件。。

Oracle Fusion Middleware 中的 Business Intelligence Enterprise Edition 的 Analytics Web General 组件存在安全漏洞。攻击者可利用该漏洞控制 Business Intelligence Enterprise Edition，影响数据的可用性、保密性和完整性。以下产品及版本受到影响：Business Intelligence Enterprise Edition 5.5.0.0.0 版本，11.1.1.9.0 版本，12.2.1.3.0 版本，12.2.1.4.0 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://www.oracle.com/security-alerts/cpuapr2020.html

6. 多款 Samsung 产品缓冲区错误漏洞（CNNVD-202004-593）

Samsung Galaxy S6 等都是韩国三星（Samsung）公司的一款智能手机。

多款 Samsung 产品（搭载 Shannon333 芯片组）中的 baseband 进程存在缓冲区错误漏洞。攻击者可通过虚假的基站推送恶意代码利用该漏洞执行代码。以下产品及版本受到影响：Samsung Galaxy S6；Galaxy S6 Edge；Galaxy S6 Edge+；Galaxy Note5。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://security.samsungmobile.com/securityUpdate.smsb

7. Apache Heron 代码问题漏洞（CNNVD-202004-1325）

Apache Heron 是一款分布式、具有容错功能的实时流处理引擎。

Apache Heron 0.20.2-incubating 版本、0.20.1-incubating 版本和 0.20.0-incubating 版本中存在代码问题漏洞。攻击者可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://lists.apache.org/thread.html/r16dd39f4180e4443ef4ca774a3a5a3d7ac69f91812c183ed2a99e959%40%3Cdev.heron.apache.org%3E

8. 多款 NETGEAR 产品 SQL 注入漏洞（CNNVD-202004-1341）

NETGEAR R6400 等都是美国网件（NETGEAR）公司的一款无线路由器。

多款 NETGEAR 产品中存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令。以下产品及版本受到影响：NETGEAR D3600 1.0.0.68 之前版本；D6000 1.0.0.68 之前版本；D6200 1.1.00.28 之前版本；D6220 1.0.0.40 之前版本；D6400 1.0.0.74 之前版本；D7000 1.0.1.60

之前版本；D7000v2 1.0.0.74 之前版本；D7800 1.0.1.34 之前版本；D8500 1.0.3.39 之前版本；DC112A 1.0.0.40 之前版本；EX8000 1.0.0.118 之前版本；JR6150 1.0.1.18 之前版本；R6050 1.0.1.18 之前版本；R6220 1.1.0.66 之前版本；R6250 1.0.4.26 之前版本；R6300v2 1.0.4.24 之前版本；R6400 1.0.1.36 之前版本；R6400v2 1.0.2.52 之前版本；R6700 1.0.1.44 之前版本；R6700v2 1.2.0.16 之前版本；R6800 1.2.0.16 之前版本；R6900v2 1.2.0.16 之前版本；R6900 1.0.1.44 之前版本；R7000 1.0.9.26 之前版本；R6900P 1.3.0.20 之前版本；R7000P 1.3.0.20 之前版本；R7100LG 1.0.0.40 之前版本；R7300DST 1.0.0.62 之前版本；R7500 1.0.0.118 之前版本；R7500v2 1.0.3.26 之前版本；R7800 1.0.2.40 之前版本；R7900 1.0.2.10 之前版本；R8000 1.0.4.12 之前版本；R7900P 1.3.0.10 之前版本；R8000P 1.3.0.10 之前版本；R8300 1.0.2.116 之前版本；R8500 1.0.2.116 之前版本；R8900 1.0.3.6 之前版本；R9000 1.0.3.10 之前版本；WNDR3700v4 1.0.2.102 之前版本；WNDR3700v5 1.1.0.54 之前版本；WNDR4300v1 1.0.2.98 之前版本；WNDR4300v2 1.0.0.56 之前版本；WNDR4500v3 1.0.0.56 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/000061197/Security-Advisory-for-SQL-Injection-on-Some-Routers-Gateways-and-Extenders-PSV-2017-3056

1.4.2 高危漏洞实例

本月高危漏洞共 873 个，其中重点漏洞实例如表 6 所示。

表 6 2020 年 4 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	资源管理错误	CNNVD-202004-1659	VMware	Google Chrome WebAudio 组件资源管理错误漏洞
		CNNVD-202004-1937	Teeworlds 团队	
		CNNVD-202004-1338	Schneider Electric	
		CNNVD-202004-423	Samsung	
		CNNVD-202004-424		
		CNNVD-202004-426		
		CNNVD-202004-223	Qualcomm	
		CNNVD-202004-283		
		CNNVD-202004-371		
		CNNVD-202004-1422	ntp	
		CNNVD-202004-126	Mozilla 基金会	
		CNNVD-202004-127		
		CNNVD-202004-544	libssh 团队	
		CNNVD-202004-1952	libslirp 项目	
		CNNVD-202004-521	Juniper Networks	
		CNNVD-202004-038	Google	
		CNNVD-202004-040		
		CNNVD-202004-193		
		CNNVD-202004-626		
		CNNVD-202004-633		
		CNNVD-202004-634		
		CNNVD-202004-647		
		CNNVD-202004-648		
		CNNVD-202004-1857		
		CNNVD-202004-2228		
		CNNVD-202004-2229		
		CNNVD-202004-002	GNU 计划	
		CNNVD-202004-1397	Foxit	
		CNNVD-202004-1398		
		CNNVD-202004-1404		
		CNNVD-202004-1405		
		CNNVD-202004-1822	Flexera Software	
		CNNVD-202004-125	Dell	
		CNNVD-202004-131		
		CNNVD-202004-1455	Autodesk	

		CNNVD-202004-2226	Apache 软件基金会	
2	注入	CNNVD-202004-174	Auth0	Microsoft Windows 和 Windows Server 注入漏洞
		CNNVD-202004-555	Dropwizard 团队	
		CNNVD-202004-598	LG	
		CNNVD-202004-610	Microsoft	
		CNNVD-202004-763		
		CNNVD-202004-916	NETGEAR	
		CNNVD-202004-1179		
		CNNVD-202004-1206		
		CNNVD-202004-1227		
		CNNVD-202004-1231		
		CNNVD-202004-1331		
		CNNVD-202004-1425		
		CNNVD-202004-1626		
		CNNVD-202004-1818		
		CNNVD-202004-1821		
		CNNVD-202004-1891		
		CNNVD-202004-1892		
		CNNVD-202004-1894		
		CNNVD-202004-1907		
		CNNVD-202004-1910		
		CNNVD-202004-1921		
		CNNVD-202004-1963		
		CNNVD-202004-1995		
		CNNVD-202004-2000	Opmantek	
		CNNVD-202004-2002	Samsung	
		CNNVD-202004-2018		
		CNNVD-202004-2248	Schneider Electric	
		CNNVD-202004-2279	WebToffee	
		CNNVD-202004-2491	Wireshark 团队	
3	信息泄露	CNNVD-202004-138	ZOHO	CIPPlanner CIPAce 信息泄露漏洞
		CNNVD-202004-170	CIPPlanner	
		CNNVD-202004-173		
		CNNVD-202004-175		
		CNNVD-202004-176		
		CNNVD-202004-181		
		CNNVD-202004-183		
		CNNVD-202004-411	Samsung	
		CNNVD-202004-434		
		CNNVD-202004-440		
		CNNVD-202004-458		
		CNNVD-202004-462		

		CNNVD-202004-470		
		CNNVD-202004-474		
		CNNVD-202004-491	GitLab	
		CNNVD-202004-538	Varnish Cache 项目	
		CNNVD-202004-596	Dell	
		CNNVD-202004-600	Samsung	
		CNNVD-202004-619	Media Library Assistant 项目	
		CNNVD-202004-660	SAP	
		CNNVD-202004-917	Microsoft	
		CNNVD-202004-1062	Oracle	
		CNNVD-202004-1096	GitLab	
		CNNVD-202004-1097		
		CNNVD-202004-1120	Broadcom	
		CNNVD-202004-1151	Draytek	
		CNNVD-202004-1237	NETGEAR	
		CNNVD-202004-1243		
		CNNVD-202004-1278		
		CNNVD-202004-1279		
		CNNVD-202004-1280		
		CNNVD-202004-2031		
		CNNVD-202004-1335	Schneider Electric	
		CNNVD-202004-1414	IBM	
		CNNVD-202004-1661	ZOHO	
		CNNVD-202004-1853	MediaWiki 基金会	
		CNNVD-202004-1870	JetBrains	
		CNNVD-202004-1971	SHARP	
		CNNVD-202004-2136	Linux 基金会	
		CNNVD-202004-2162	Percona	
		CNNVD-202004-2355	LCDS	
4	输入验证错误	CNNVD-202004-1828	Vesta Control Panel	Microsoft Office 输入验证错误漏洞
		CNNVD-202004-539	Varnish Cache 项目	
		CNNVD-202004-1254	Squid	
		CNNVD-202004-672	SAP	
		CNNVD-202004-241	Samsung	
		CNNVD-202004-247		
		CNNVD-202004-264		
		CNNVD-202004-298		
		CNNVD-202004-327		
		CNNVD-202004-330		
		CNNVD-202004-333		
		CNNVD-202004-338		

		CNNVD-202004-342		
		CNNVD-202004-480		
		CNNVD-202004-1807	Red Hat	
		CNNVD-202004-220	Qualcomm	
		CNNVD-202004-234		
		CNNVD-202004-1925	Plex	
		CNNVD-202004-1232	NETGEAR	
		CNNVD-202004-1236		
		CNNVD-202004-1271		
		CNNVD-202004-1829		
		CNNVD-202004-1897		
		CNNVD-202004-697	Microsoft	
		CNNVD-202004-785		
		CNNVD-202004-503	Juniper Networks	
		CNNVD-202004-523		
		CNNVD-202004-527		
		CNNVD-202004-530		
		CNNVD-202004-1873	JetBrains	
		CNNVD-202004-1953		
		CNNVD-202004-759	IBM	
		CNNVD-202004-803	Git	
		CNNVD-202004-1786		
		CNNVD-202004-2465	F5	
		CNNVD-202004-554	Dahua	
		CNNVD-202004-368	cross domain local storage 项目	
		CNNVD-202004-369		
		CNNVD-202004-1101	Cisco	
		CNNVD-202004-1106		
		CNNVD-202004-1108		
		CNNVD-202004-2394	Cerner	
		CNNVD-202004-024	Avast	
		CNNVD-202004-026		
		CNNVD-202004-1264	Arista Networks	
5	跨站请求伪造	CNNVD-202004-008	Auth0	Foxit Reader 和 PhantomPDF communication API 跨站请求伪造漏洞
		CNNVD-202004-395	PrimeKey Solutions	
		CNNVD-202004-409	Plat’ Home	
		CNNVD-202004-942	Fraction	
		CNNVD-202004-1381	Foxit	
		CNNVD-202004-1383		
		CNNVD-202004-1613	NETGEAR	
		CNNVD-202004-1619		
		CNNVD-202004-1625		

		CNNVD-202004-1816		
		CNNVD-202004-1879		
		CNNVD-202004-1886		
		CNNVD-202004-1887		
		CNNVD-202004-1914		
		CNNVD-202004-1917		
		CNNVD-202004-1928		
		CNNVD-202004-1983		
		CNNVD-202004-1990		
		CNNVD-202004-2006		
		CNNVD-202004-2039		
		CNNVD-202004-2097		
		CNNVD-202004-2123		
		CNNVD-202004-2185		
		CNNVD-202004-1275		
		CNNVD-202004-2489	Apache 软件基金会	
		CNNVD-202004-1964	Supsystic	
		CNNVD-202004-2045	IBM	
6	缓冲区错误	CNNVD-202004-656	英国剑桥大学	Adobe Bridge 缓冲区错误漏洞
		CNNVD-202004-947	Triangle MicroWorks	
		CNNVD-202004-953		
		CNNVD-202004-081	TP-Link	
		CNNVD-202004-284	Solarwinds	
		CNNVD-202004-237	Samsung	
		CNNVD-202004-238		
		CNNVD-202004-314		
		CNNVD-202004-271		
		CNNVD-202004-346		
		CNNVD-202004-197	Qualcomm	
		CNNVD-202004-217		
		CNNVD-202004-218		
		CNNVD-202004-222		
		CNNVD-202004-224		
		CNNVD-202004-258		
		CNNVD-202004-265		
		CNNVD-202004-301		
		CNNVD-202004-331		
		CNNVD-202004-1407	PHP	
		CNNVD-202004-499	Palo Alto Networks	
		CNNVD-202004-1977	Ntop	
		CNNVD-202004-1204	NETGEAR	
		CNNVD-202004-1229		

		CNNVD-202004-1246		
		CNNVD-202004-1266		
		CNNVD-202004-1267		
		CNNVD-202004-1268		
		CNNVD-202004-1269		
		CNNVD-202004-1270		
		CNNVD-202004-1281		
		CNNVD-202004-1345		
		CNNVD-202004-1350		
		CNNVD-202004-1364		
		CNNVD-202004-1369		
		CNNVD-202004-1883		
		CNNVD-202004-1932		
		CNNVD-202004-1986		
		CNNVD-202004-1992		
		CNNVD-202004-1994		
		CNNVD-202004-1996		
		CNNVD-202004-2029		
		CNNVD-202004-2033		
		CNNVD-202004-2036		
		CNNVD-202004-2089		
		CNNVD-202004-2090		
		CNNVD-202004-2091		
		CNNVD-202004-2105		
		CNNVD-202004-2106		
		CNNVD-202004-2107		
		CNNVD-202004-2108		
		CNNVD-202004-2110		
		CNNVD-202004-2111		
		CNNVD-202004-2112		
		CNNVD-202004-2113		
		CNNVD-202004-2114		
		CNNVD-202004-2116		
		CNNVD-202004-2117		
		CNNVD-202004-2172		
		CNNVD-202004-2206		
		CNNVD-202004-2212		
		CNNVD-202004-2217		
		CNNVD-202004-2218		
		CNNVD-202004-2219		
		CNNVD-202004-2220		
		CNNVD-202004-2240		

		CNNVD-202004-2268		
		CNNVD-202004-2270		
		CNNVD-202004-2271		
		CNNVD-202004-2274		
		CNNVD-202004-2275		
		CNNVD-202004-2277		
		CNNVD-202004-2282		
		CNNVD-202004-2283		
		CNNVD-202004-2284		
		CNNVD-202004-2285		
		CNNVD-202004-2287		
		CNNVD-202004-2290		
		CNNVD-202004-2293		
		CNNVD-202004-2295		
		CNNVD-202004-2296		
		CNNVD-202004-2297		
		CNNVD-202004-2299		
		CNNVD-202004-2313		
		CNNVD-202004-2315		
		CNNVD-202004-2316		
		CNNVD-202004-2319		
		CNNVD-202004-320	Mozilla 基金会	
		CNNVD-202004-336		
		CNNVD-202004-340		
		CNNVD-202004-688	Microsoft	
		CNNVD-202004-689		
		CNNVD-202004-691		
		CNNVD-202004-692		
		CNNVD-202004-693		
		CNNVD-202004-694		
		CNNVD-202004-695		
		CNNVD-202004-698		
		CNNVD-202004-705		
		CNNVD-202004-710		
		CNNVD-202004-733		
		CNNVD-202004-734		
		CNNVD-202004-740		
		CNNVD-202004-743		
		CNNVD-202004-744		
		CNNVD-202004-746		
		CNNVD-202004-748		
		CNNVD-202004-764		

		CNNVD-202004-765		
		CNNVD-202004-766		
		CNNVD-202004-768		
		CNNVD-202004-769		
		CNNVD-202004-770		
		CNNVD-202004-771		
		CNNVD-202004-773		
		CNNVD-202004-774		
		CNNVD-202004-775		
		CNNVD-202004-776		
		CNNVD-202004-792		
		CNNVD-202004-793		
		CNNVD-202004-794		
		CNNVD-202004-804		
		CNNVD-202004-141	Linux 基金会	
		CNNVD-202004-1440	LG	
		CNNVD-202004-1095	Intel	
		CNNVD-202004-061	Huawei	
		CNNVD-202004-1966		
		CNNVD-202004-1967		
		CNNVD-202004-1969		
		CNNVD-202004-069	HAProxy	
		CNNVD-202004-194	Google	
		CNNVD-202004-195		
		CNNVD-202004-646		
		CNNVD-202004-033		
		CNNVD-202004-649		
		CNNVD-202004-1859		
		CNNVD-202004-001	GNU 计划	
		CNNVD-202004-374	Fuji Electric	
		CNNVD-202004-1391	Foxit	
		CNNVD-202004-1393		
		CNNVD-202004-1394		
		CNNVD-202004-1395		
		CNNVD-202004-1396		
		CNNVD-202004-1400		
		CNNVD-202004-1402		
		CNNVD-202004-625	Cypress Semiconductor	
		CNNVD-202004-1104	Cisco	
		CNNVD-202004-1105		
		CNNVD-202004-2395	Cerner	

		CNNVD-202004-2396		
		CNNVD-202004-2397		
		CNNVD-202004-2480	BMC Software	
		CNNVD-202004-023	Avast	
		CNNVD-202004-1454	Autodesk	
		CNNVD-202004-1459		
		CNNVD-202004-964	Adobe	
		CNNVD-202004-2278		
		CNNVD-202004-2280		
		CNNVD-202004-2288		
		CNNVD-202004-2292		
		CNNVD-202004-2294		
		CNNVD-202004-2301		
		CNNVD-202004-2302		
		CNNVD-202004-2305		
		CNNVD-202004-2309		
		CNNVD-202004-2310		
		CNNVD-202004-2314		
		CNNVD-202004-2322		
7	代码问题	CNNVD-202004-1469	WSO2	Microsoft SharePoint 代码问题漏洞
		CNNVD-202004-013	TP-Link	
		CNNVD-202004-1612	TOSHIBA	
		CNNVD-202004-123	TestLink 团队	
		CNNVD-202004-365	Synergy Systems & Solutions	
		CNNVD-202004-1147	SilverStripe	
		CNNVD-202004-1947	Schneider Electric	
		CNNVD-202004-680	SAP	
		CNNVD-202004-272	Samsung	
		CNNVD-202004-296		
		CNNVD-202004-312		
		CNNVD-202004-313		
		CNNVD-202004-1862	Red Hat	
		CNNVD-202004-232	Qualcomm	
		CNNVD-202004-399	PrimeKey Solutions	
		CNNVD-202004-1790	OpenSSL 团队	
		CNNVD-202004-1406	OPC Foundation	
		CNNVD-202004-704	Microsoft	
		CNNVD-202004-707		
		CNNVD-202004-709		
		CNNVD-202004-713		
		CNNVD-202004-714		

		CNNVD-202004-720		
		CNNVD-202004-165	Malwarebytes	
		CNNVD-202004-562	Linux 基金会	
		CNNVD-202004-1452	LG	
		CNNVD-202004-939	Lenovo	
		CNNVD-202004-1871	JetBrains	
		CNNVD-202004-1951		
		CNNVD-202004-350	HCL Technologies	
		CNNVD-202004-190	Google	
		CNNVD-202004-1813		
		CNNVD-202004-1820	Flexera Software	
		CNNVD-202004-1133	dom4j 项目	
		CNNVD-202004-1327	CloudBees	
		CNNVD-202004-1328		
		CNNVD-202004-1329		
		CNNVD-202004-1451	Autodesk	
		CNNVD-202004-1453		
		CNNVD-202004-383	Advantech	
8	操作系统命令注入	CNNVD-202004-380	Advantech	NETGEAR WAC505 和 WAC510 操作系统命令注入漏洞
		CNNVD-202004-599	D-Link	
		CNNVD-202004-623	Rubrik	
		CNNVD-202004-1150	Dell	
		CNNVD-202004-1285	NETGEAR	
		CNNVD-202004-1286		
		CNNVD-202004-1287		
		CNNVD-202004-1288		
		CNNVD-202004-1289		
		CNNVD-202004-1290		
		CNNVD-202004-1291		
		CNNVD-202004-1292		
		CNNVD-202004-1293		
		CNNVD-202004-1294		
		CNNVD-202004-1295		
		CNNVD-202004-1372		
		CNNVD-202004-1923		
		CNNVD-202004-1938		
		CNNVD-202004-1941		
		CNNVD-202004-2004		
		CNNVD-202004-2037		
		CNNVD-202004-2196		
		CNNVD-202004-2198		
		CNNVD-202004-2199	Opmantek	

		CNNVD-202004-2482 CNNVD-202004-2485	BMC Software	

1. Google Chrome WebAudio 组件资源管理错误漏洞

（CNNVD-202004-038）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。WebAudio 是其中的一个音频组件。

Google Chrome 80.0.3987.162 之前版本中的 WebAudio 组件存在资源管理错误漏洞。远程攻击者可借助特制网站利用该漏洞执行任意代码或导致拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-desktop_31.html

2. Microsoft Windows 和 Windows Server 注入漏洞

（CNNVD-202004-763）

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。

Microsoft Windows 和 Windows Server 中存在安全漏洞，该漏洞源于程序没有正确处理令牌对象。攻击者可利用该漏洞绕过沙盒保护。以下产品及版本受到影响：Microsoft Windows 10 1903 版本，Windows 10 1909 版本，Windows Server 1903 版本，Windows Server 1909 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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0981

3. CIPPlanner CIPAce 信息泄露漏洞（CNNVD-202004-2136）

helm 是一款 Kubernetes 包管理器。

helm 3.1.0 版本至 3.1.2 版本中存在信息泄露漏洞。攻击者可利用该漏洞获取对集群的查询信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/helm/helm/security/advisories/GHSA-q8q8-93cv-v6h8

4. Microsoft Office 输入验证错误漏洞（CNNVD-202004-697）

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 中存在安全漏洞。攻击者可借助特制的 Office 文档利用该漏洞安装程序，查看、更改或删除数据及创建拥有全部用户权限的帐户。以下产品及版本受到影响：Microsoft Access 2010 SP2，Microsoft Access 2013 SP1，Microsoft Access 2016；Microsoft Excel 2010 SP2，Microsoft Excel 2013 RT SP1，Microsoft Excel 2013 SP1，Microsoft Excel 2016；Microsoft Office 2010 SP2，Microsoft Office 2013 RT SP1，Microsoft Office 2013 SP1，Microsoft Office 2016，Microsoft Office 2019，Office 365 ProPlus；Microsoft

Outlook 2010 SP2，Microsoft Outlook 2013 RT SP1，Microsoft Outlook 2013 SP1，Microsoft Outlook 2016；Microsoft PowerPoint 2010 SP2，Microsoft PowerPoint 2013 RT SP1，Microsoft PowerPoint 2013 SP1，Microsoft PowerPoint 2016；Microsoft Project 2010 SP2，Microsoft Project 2013 SP1，Microsoft Project 2016；Microsoft Publisher 2010 SP2，Microsoft Publisher 2013 SP1，Microsoft Publisher 2016；Microsoft Visio 2010 SP2，Microsoft Visio 2013 SP1，Microsoft Visio 2016；Microsoft Word 2010 SP2，Microsoft Word 2013 RT SP1，Microsoft Word 2013 SP1，Microsoft Word 2013 SP1，Microsoft Word 2016。

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-2020-0760

5. Foxit Reader 和 PhantomPDF communication API 跨站请求伪造漏洞（CNNVD-202004-1381）

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

基于 Windows 平台的 Foxit Reader 和 Foxit PhantomPDF 9.7.1.29511 及之前版本中的 communication API 存在跨站请求伪造漏洞。攻击者可借助恶意的文件或页面利用该漏洞在当前进程的上下文中执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

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

6. Adobe Bridge 缓冲区错误漏洞（CNNVD-202004-2301）

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。

基于 Windows 平台的 Adobe Bridge 10.0.1 及之前版本中存在缓冲区错误漏洞。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://helpx.adobe.com/security/products/bridge/apsb20-19.html

7. Microsoft SharePoint 代码问题漏洞（CNNVD-202004-704）

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 Enterprise Server 2016 和 Microsoft SharePoint Server 2019 中存在安全漏洞。攻击者可利用该漏洞在 SharePoint 应用程序池和 SharePoint 服务器场帐户的上下文中运行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0974

8. NETGEAR WAC505 和 WAC510 操作系统命令注入漏洞（CNNVD-202004-1923）

NETGEAR WAC505 和 NETGEAR WAC510 都是美国网件（NETGEAR）公司的一款无线接入点（AP）。

NETGEAR WAC505 5.0.0.17 之前版本和 WAC510 5.0.0.17 之前

版本中存在操作系统命令注入漏洞。该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令等。攻击者可利用该漏洞执行非法操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://kb.netgear.com/000060232/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-Wireless-Access-Points-PSV-2018-0262

二、接报漏洞情况

本月接报漏洞 9607 个，其中信息技术产品漏洞（通用型漏洞）285 个，网络信息系统漏洞（事件型漏洞）9322 个。

表 7 2020 年 4 月漏洞接报情况

序号	报送单位	漏洞总量
1	上海斗象信息科技有限公司	4562
2	网神信息技术（北京）股份有限公司	3646
3	内蒙古洞明科技有限公司	330
4	太极计算机股份有限公司	253
5	北京华云安信息技术有限公司	239
6	北京奇虎科技有限公司	161
7	北京启明星辰信息安全技术有限公司	63
8	远江盛邦(北京)网络安全科技股份有限公司	52
9	西安四叶草信息科技有限公司	37
10	中国电信集团系统集成有限责任公司	33

11	绿盟科技集团股份有限公司安全研究部	30
12	山东新潮信息技术有限公司	25
13	星云博创科技有限公司	20
14	四叶草信息技术有限公司	20
15	北京圣溥润高新技术服份有限公司	20
16	杭州安恒信息技术股份有限公司	15
17	南京铱迅信息技术股份有限公司	12
18	浙江宇视科技有限公司	10
19	个人	8
20	上海安识网络科技有限公司	6
21	天津市兴先道科技有限公司	5
22	西安交大捷普网络科技有限公司	5
23	郑州大学	4
24	北京天融信网络安全技术有限公司	4
25	北京智游网安科技有限公司	4
26	上海交通大学网络安全与隐私保护实验室（NSEC lab）	4
27	北京长亭科技有限公司	4
28	北京山石网科信息技术有限公司	4
29	中兴通讯	3
30	上海安洵信息技术有限公司	3
31	长扬科技（北京）有限公司	3
32	北京知道创宇信息技术股份有限公司	3
33	北京威努特技术有限公司	2

34	北京江南天安科技有限公司	2
35	云南瑞讯达通信技术有限公司	2
36	上海谋乐网络科技有限公司	2
37	北京安赛创想科技有限公司	2
38	中国工商银行安全攻防实验室	2
39	广州天懋信息系统股份有限公司	1
40	湖南亚防科技有限公司	1
41	北京神州绿盟科技有限公司	1
42	北京邮电大学	1
43	北京智游网安科技有限公司	1
44	北京微步在线科技有限公司	1
45	北京网思科平科技有限公司	1
报送总计		9607

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，包括 Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202004-785、CVE-2020-0938）、Microsoft Excel 安全漏洞（CNNVD-202004-710、CVE-2020-0979 ）、Microsoft SharePoint 安全漏洞（CNNVD-202004-720、CVE-2020-0920）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

本次漏洞公告涉及 Windows 系统、Adobe Type 字体库、Microsoft Office、Microsoft 图形组件、Windows SMBv3 客户端等 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，漏洞详情如下：

1、Microsoft Windows 和 Windows Server 安全漏洞（CNNVD-202004-785、CVE-2020-0938）（CNNVD-202003-1524、CVE-2020-1020）

漏洞简介：当 Windows Adobe Type Manager 库未正确处理经特殊设计的 Adobe Type 1 PostScript 格式字体时，会触发远程代码执行漏洞。对于除 Windows 10 之外的所有系统，成功利用此漏洞的攻击者可以远程执行代码。对于运行 Windows 10 的系统，成功利用此漏洞的攻击者可以利用受限的特权和功能在 AppContainer 沙盒的上下文中执行代码。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 Dynamics Business Central 安全漏洞（CNNVD-202004-916、CVE-2020-1022）

漏洞简介：Microsoft Dynamics Business Central 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在目标服务器上执行任意代码。

3、MICROSOFT WINDOWS GRAPHICS DEVICE INTERFACE 安全漏洞（CNNVD-202004-765、CVE-2020-0964）

漏洞简介： Windows 图形设备接口 (GDI) 处理内存中对象的方式时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。

4、Microsoft Excel 安全漏洞（CNNVD-202004-710、CVE-2020-0979）（CNNVD-202004-694、CVE-2020-0906）

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。

5、Microsoft Office 安全漏洞（CNNVD-202004-697、CVE-2020-0760）（CNNVD-202004-705、CVE-2020-0991）

漏洞简介：当 Microsoft Office 不正确地加载任意类型的库时，会触发远程代码执行漏洞。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。

6、Microsoft SharePoint 安全漏洞（CNNVD-202004-720、

CVE-2020-0920 ）（ CNNVD-202004-713 、 CVE-2020-0931 ）（CNNVD-202004-709、CVE-2020-0932）（ CNNVD-202004-704 、 CVE-2020-0974 ）（ CNNVD-202004-714 、CVE-2020-0929）（CNNVD-202004-707、CVE-2020-0971）

漏洞简介：当 Microsoft SharePoint 无法检查应用程序包的源标记时，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 SharePoint 应用程序池和 SharePoint 服务器帐户的上下文中运行任意代码。

7、Microsoft Word 安全漏洞（CNNVD-202004-698、CVE-2020-0980）

漏洞简介：当 Microsoft Word 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。

8 、 Microsoft Windows Graphics Components 安全漏洞（ CNNVD-202004-792 、 CVE-2020-0907 ）（ CNNVD-202004-804 、CVE-2020-0687）

漏洞简介：Microsoft 图形组件在内存中处理对象的方式存在远程代码执行漏洞。成功利用该漏洞的攻击者可以对目标系统执行任意代码。若要利用该漏洞，攻击者需要诱使用户打开一个经特殊设计的文件。

9、Microsoft Windows Hyper-V 安全漏洞（CNNVD-202004-793、CVE-2020-0910）

漏洞简介：当主机服务器上的 Windows Hyper-V 无法正确验证来宾操作系统上经身份验证的用户输入时，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主机操作系统上执行任意代码。

10、Microsoft Office 安全漏洞（CNNVD-202004-695、CVE-2020-0961）

漏洞简介：当 Windows Office 访问连接引擎不能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目标系统上执行任意代码。攻击者可以通过诱使目标打开经特殊设计的文件来利用此漏洞。

11、Microsoft Server Message Block 安全漏洞（CNNVD-202003-607、CVE-2020-0796）

漏洞简介：Microsoft 服务器消息块 3.1.1 (SMBv3) 协议处理某些请求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以在目标服务器或客户端上执行任意代码。

12 、 Microsoft Windows Media Foundation 安 全 漏 洞 （CNNVD-202004-776、CVE-2020-0948）（CNNVD-202004-775、CVE-2020-0949）（CNNVD-202004-774、CVE-2020-0950）

漏洞简介：当 Microsoft Windows Media Foundation 不正确地处理内存中对象时，会触发内存损坏漏洞。成功利用此漏洞的攻击者可以安装程序；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。攻击者可能通过多种方式利用此漏洞，包括诱使用户打开经特殊设计的文档或诱使用户访问恶意网页。

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 Windows 和 Windows Server 安全漏洞（CNNVD-202004-785、CVE-2020-0938）（CNNVD-202003-1524、CVE-2020-1020）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0938 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020
2	Microsoft Dynamics Business Central 安全漏洞（CNNVD-202004-916、CVE-2020-1022）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1022
3	MICROSOFT WINDOWS GRAPHICS DEVICE INTERFACE 安全漏洞（CNNVD-202004-765、CVE-2020-0964）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0964
4	Microsoft Excel 安全漏洞（CNNVD-202004-710、CVE-2020-0979）（CNNVD-202004-694、CVE-2020-0906）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0979 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0906
5	Microsoft Office 安全漏洞（CNNVD-202004-697、CVE-2020-0760）（CNNVD-202004-705、CVE-2020-0991）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0760 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0991
6	Microsoft SharePoint 安全漏洞（CNNVD-202004-720、CVE-2020-0920）（CNNVD-202004-713、CVE-2020-0931）（CNNVD-202004-709、CVE-2020-0932）（CNNVD-202004-704、CVE-2020-0974）（CNNVD-202004-714、CVE-2020-0929）（CNNVD-202004-707、CVE-2020-0971）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0920 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0931 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0932 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0974 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0929 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0971
7	Microsoft Word 安全漏洞（CNNVD-202004-698、CVE-2020-0980）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0980
8	Microsoft Windows Graphics Components 安全漏洞（CNNVD-202004-792、CVE-2020-0907）（CNNVD-202004-804、CVE-2020-0687）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0907 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0687

9	Microsoft Windows Hyper-V 安全漏洞（CNNVD-202004-793、CVE-2020-0910）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0910
10	Microsoft Office 安全漏洞（CNNVD-202004-695、CVE-2020-0961）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0961
11	Microsoft Server Message Block 安全漏洞（CNNVD-202003-607、CVE-2020-0796）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0796
12	Microsoft Windows Media Foundation 安全漏洞（CNNVD-202004-776、CVE-2020-0948）（CNNVD-202004-775、CVE-2020-0949）（CNNVD-202004-774、CVE-2020-0950）	https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0948 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0949 https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-0950

3.2 通达 OA 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于通达 OA 安全漏洞（CNNVD-202004-1959）的报送。成功利用该漏洞的攻击者可以任意登录账户，控制通达 OA 系统。通达 OA v11.5.200417 之前版本均受此漏洞影响。目前，通达 OA 官方网站已发布新版本修复了该漏洞，请用户及时确认系统版本，尽快采取修补措施。

.漏洞介绍

通达 OA（Office Anywhere 网络智能办公系统）是由北京通达信科科技有限公司自主研发的协同办公自动化软件。其用户主要是中国国内，包括军队、公安、电力、电信等重要机构。

漏洞源于系统对用户传入数据过滤不严，导致攻击者可以伪造任意帐户登录系统。未经授权的攻击者可以通过精心构造的 HTTP 请求登录任意用户，包括 Admin 用户，从而控制通达 OA 系统，甚至有可能结合其它漏洞控制整个服务器。

.危害影响

成功利用该漏洞的攻击者可以任意登录账户，控制通达 OA 系统。通达 OA v11.5.200417 之前版本均受此漏洞影响。

.修复建议

目前，通达 OA 官方网站已发布新版本修复了该漏洞，请用户及时确认系统版本，尽快采取修补措施。官方更新链接如下：

https://www.tongda2000.com/download/sp2019.php