北京师范大学网络信息安全通告

2021 年 5 月报告

北京师范大学信息网络中心

2021 年 6 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，2021 年 5 月份新增安全漏洞共 1682 个，从厂商分布来看，Google 公司产品的漏洞数量最多，共发布 171 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 13.91%。本月新增漏洞中，超危漏洞 159 个、高危漏洞 617 个、中危漏洞 823 个、低危漏洞 80 个，相应修复率分别为 74.21%、91.57%、86.76%以及 86.25%。合计 1466 个漏洞已有修复补丁发布，本月整体修复率 87.31%。

截至 2021 年 05 月 31 日，CNNVD 采集漏洞总量已达 163828 个。

1.1 漏洞增长概况

2021 年 5 月新增安全漏洞 1682 个，与上月（1880 个）相比减少了 10.53%。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 1607 个。

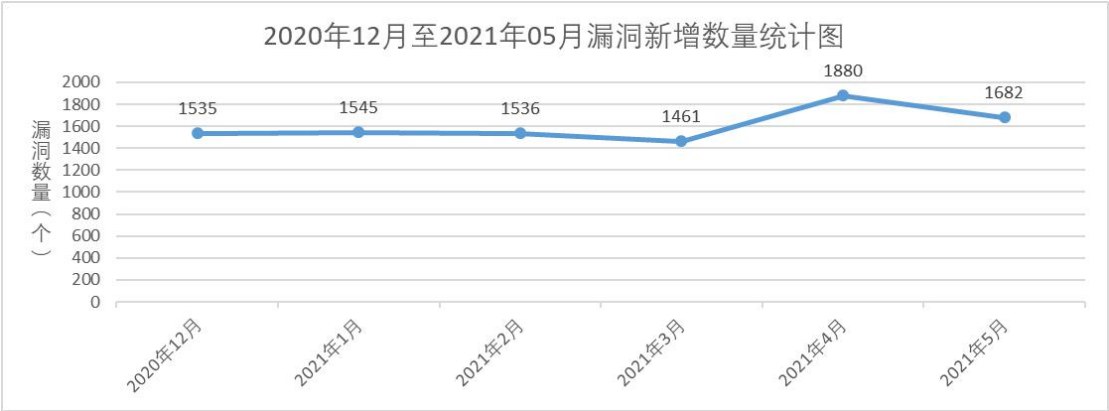

图 1 2020 年 12 月至 2021 年 5 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

5 月厂商漏洞数量分布情况如表 1 所示，Google 公司漏洞达到 171 个，占本月漏洞总量的 10.17%。

表 1　2021 年 5 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（个）	所占比例
1	Google	171	10.17%
2	WordPress 基金会	82	4.88%
3	Apple	77	4.58%
4	IBM	74	4.40%
5	Microsoft	61	3.63%
6	Cisco	60	3.57%
7	Adobe	42	2.50%
8	Foxit	35	2.08%
9	Linux 基金会	33	1.96%
10	JetBrains	28	1.66%

1.2.2 漏洞产品分布

5 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 22 个，占主流操作系统漏洞总量的 16.42%，排名第一。

表 2　2021 年 5 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	22
2	Windows Server 2019	13
3	Windows Server 2016	9
4	Windows Server 2012	9
5	Windows Server 2012 R2	9
6	Windows 8.1	9
7	Windows Rt 8.1	8
8	Windows Server 2008	7
9	Windows Server 2008 R2	7

10	Windows 7	8
11	Android	27
12	Linux Kernel	6

1.2.3 漏洞类型分布

5 月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 13.91%。

表 3 2021 年 5 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	234	13.91%
2	跨站脚本	194	11.53%
3	代码问题	105	6.24%
4	输入验证错误	86	5.11%
5	资源管理错误	86	5.11%
6	信息泄露	65	3.86%
7	授权问题	48	2.85%
8	数字错误	40	2.38%
9	权限许可和访问控制问题	37	2.20%
10	命令注入	36	2.14%
11	跨站请求伪造	33	1.96%
12	SQL 注入	28	1.66%
13	访问控制错误	26	1.55%
14	路径遍历	26	1.55%
15	操作系统命令注入	25	1.49%
16	安全特征问题	24	1.43%
17	信任管理问题	22	1.31%
18	代码注入	20	1.19%
19	注入	11	0.65%
20	加密问题	10	0.59%
21	竞争条件问题	7	0.42%
22	数据伪造问题	5	0.30%
23	参数注入	3	0.18%
24	日志信息泄露	2	0.12%
25	后置链接	1	0.06%
26	格式化字符串错误	1	0.06%
27	环境问题	1	0.06%
28	配置错误	1	0.06%
29	**其他**	505	30.02%

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。5 月漏洞危害等级分布如图 2 所示，其中超危漏洞 159 条，占本月漏洞总数的 9.47%。

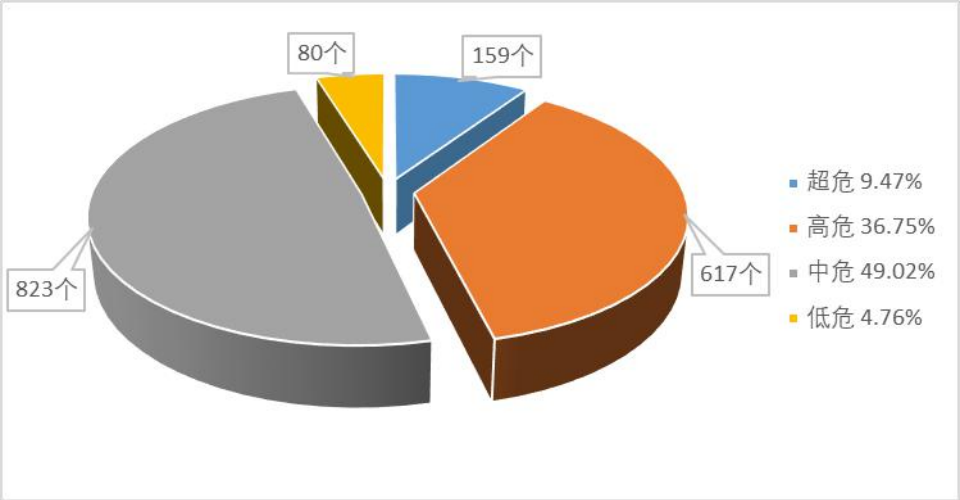

图 2　2021 年 5 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

5 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 91.57%，超危漏洞修复率最低，比例为 74.21%。

总体来看，本月整体修复率，由上月的 88.62%下降至本月的 87.31%。

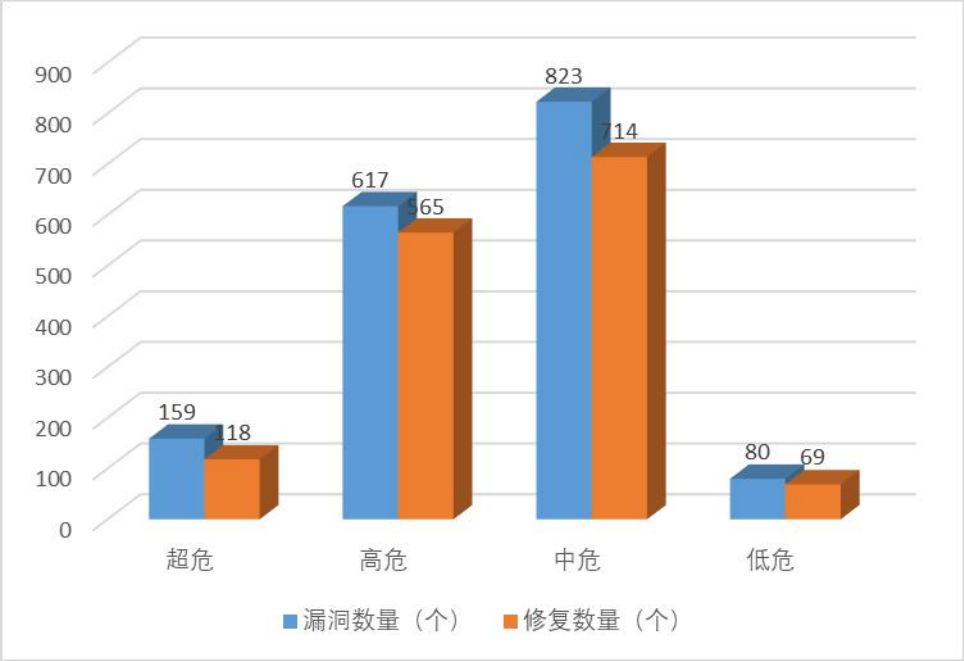

图 3　2021 年 5 月漏洞修复数量统计

1.3.2　厂商修复情况

5 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Google、WordPress 基金会、Apple 等十个厂商共 663 条漏洞，占本月漏洞总数的 39.42%，漏洞修复率为 97.89%，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 WordPress 基金会、Microsoft、Cisco、Adobe、Foxit、JetBrains 等公司本月漏洞修复率均为 100%，共 649 条漏洞已全部修复。

表 4　2021 年 5 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	171	170	99.42%
2	WordPress 基金会	82	82	100.00%
3	Apple	77	76	98.70%
4	IBM	74	66	89.19%
5	Microsoft	61	61	100.00%
6	Cisco	60	60	100.00%
7	Adobe	42	42	100.00%
8	Foxit	35	35	100.00%
9	Linux 基金会	33	29	87.88%

10	JetBrains	28	28	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 159 个，其中重要漏洞实例如表 5 所示。

表 5　2021 年 5 月超危漏洞实例

序号	漏洞类型	厂商	CNNVD 编号	漏洞实例
1	SQL 注入	Artica	CNNVD-202105-339	WordPress 插件 SQL 注入漏洞（CNNVD-202105-975）
		Control Web Panel 社区	CNNVD-202105-1229	
		KonaWiki	CNNVD-202105-795	
		Wordpress 基金会	CNNVD-202105-1146	
			CNNVD-202105-975	
		Zzcms 团队	CNNVD-202105-1491	
		个人开发者	CNNVD-202105-1470	
			CNNVD-202105-244	
			CNNVD-202105-245	
			CNNVD-202105-778	
			CNNVD-202105-242	
			CNNVD-202105-241	
			CNNVD-202105-235	
			CNNVD-202105-243	
			CNNVD-202105-857	
2	代码问题	Artica	CNNVD-202105-343	SolarWinds Network Performance Monitor 代码问题漏洞（CNNVD-202105-1314）
		BMC Software	CNNVD-202105-1274	
		Emerson	CNNVD-202105-1239	
		Golo	CNNVD-202105-779	
		KonaWiki	CNNVD-202105-794	
		Re-Logic	CNNVD-202105-1484	
		SolarWinds	CNNVD-202105-1314	
		Wordpress 基金会	CNNVD-202105-250	
			CNNVD-202105-974	
		Zebra Technologies	CNNVD-202105-709	
		个人开发者	CNNVD-202105-966	
			CNNVD-202105-834	
			CNNVD-202105-1670	

			CNNVD-202105-292	
			CNNVD-202105-1519	
			CNNVD-202105-044	
			CNNVD-202105-697	
			CNNVD-202105-239	
			CNNVD-202105-831	
3	授权问题	ASUS	CNNVD-202105-277	Cisco SD-WAN vManage Software 授权问题漏洞（CNNVD-202105-221）
		Cisco	CNNVD-202105-221	
		HPE	CNNVD-202105-111	
		IBM	CNNVD-202105-992	
			CNNVD-202105-1939	
		Libre Wireless	CNNVD-202105-046	
		MesaLabs	CNNVD-202105-1780	
			CNNVD-202105-1776	
4	操作系统命令注入	Cisco	CNNVD-202105-226	Cisco HyperFlex HX Data Platform 操作系统命令注入漏洞（CNNVD-202105-225）
			CNNVD-202105-225	
		JetBrains	CNNVD-202105-691	
		Netgear	CNNVD-202105-1401	
		个人开发者	CNNVD-202105-712	
			CNNVD-202105-1210	
5	缓冲区错误	3S-Smart Software Solutions	CNNVD-202105-1625	Qualcomm 组件缓冲区错误漏洞（CNNVD-202105-029）
			CNNVD-202105-1634	
			CNNVD-202105-1622	
			CNNVD-202105-1623	
		Amazon	CNNVD-202105-043	
		Gentoo 基金会	CNNVD-202105-115	
		Homebrew Formulae	CNNVD-202105-275	
		Linux 基金会	CNNVD-202105-1646	
			CNNVD-202105-1642	
		Mercedes Benz	CNNVD-202105-851	
			CNNVD-202105-852	
		Moxa	CNNVD-202105-496	
			CNNVD-202105-495	
		Pulse Secure	CNNVD-202105-1009	
		Qualcomm	CNNVD-202105-029	
		Tenda	CNNVD-202105-382	
			CNNVD-202105-380	
			CNNVD-202105-384	
			CNNVD-202105-381	
		个人开发者	CNNVD-202105-1380	
			CNNVD-202105-106	
			CNNVD-202105-1378	

			CNNVD-202105-1373	
			CNNVD-202105-176	
			CNNVD-202105-1374	
			CNNVD-202105-1386	
			CNNVD-202105-1372	
			CNNVD-202105-1376	
			CNNVD-202105-1382	
6	访问控制错误	WAGO	CNNVD-202105-829	Wordpress 基金会 themegrill-demo-importer 访问控制错误漏洞（CNNVD-202105-188）
		Wordpress 基金会	CNNVD-202105-188	
		个人开发者	CNNVD-202105-240	
7	资源管理错误	Gentoo 基金会	CNNVD-202105-095	Microsoft HTTP.sys 资源管理错误漏洞（CNNVD-202105-588）
		Microsoft	CNNVD-202105-588	
		Qualcomm	CNNVD-202105-007	
		个人开发者	CNNVD-202105-1393	
8	输入验证错误	Mercedes Benz	CNNVD-202105-850	Qualcomm 组件输入验证错误漏洞（CNNVD-202105-031）
		Metinfo	CNNVD-202105-1501	
		Qualcomm	CNNVD-202105-031	
		个人开发者	CNNVD-202105-097	
			CNNVD-202105-194	
			CNNVD-202105-119	

1. WordPress 插件 SQL 注入漏洞（CNNVD-202105-975）

WordPress 插件是 WordPress 开源的一个应用插件。

Car Seller - Auto Classifieds Script WordPress plugin 2.1.0 版本及之前版本存在 SQL 注入漏洞，身份验证和未经身份验证的用户 order_id POST 参数在 SQL 语句中使用它之前,导致 SQL 注入问题。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://wpscan.com/vulnerability/f35d6ab7-dd52-48b3-a79c-3f89edf24162

2. SolarWinds Network Performance Monitor 代码问题漏洞（CNNVD-202105-1314）

Solarwinds SolarWinds Network Performance Monitor（NPM）是

美国 SolarWinds 公司的一款网络性能监视器，它为路由器、虚拟化环境和其他设备提供监控和报告、跟踪 up/down 状态、实时分析和网络性能统计等功能。

SolarWinds Network Performance Monitor 存在安全漏洞，该漏洞允许远程攻击者在受影响的 SolarWinds 网络性能监视器安装上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://documentation.solarwinds.com/en/success_center/sam/content/release_notes/sam_2020-2-5_release_notes.htm

3. Cisco SD-WAN vManage Software 授权问题漏洞（CNNVD-202105-221）

Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。

Cisco SD-WAN vManage Cluster 存在授权问题漏洞，远程攻击者可以绕过授权检查并进行应用程序修改，可能使攻击者的权限提升受影响系统中的特权。

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-sd-wan-vmanage-4TbynnhZ

4. Cisco HyperFlex HX Data Platform 操作系统命令注入漏洞（CNNVD-202105-225）

Cisco HyperFlex HX Data Platform 是美国思科（Cisco）公司的一

个网络设备。提供企业级的敏捷性，可扩展性，安全性和生命周期管理功能。

Cisco HyperFlex HX Data Platform 存在操作系统命令注入漏洞，该漏洞允许未经身份验证的远程攻击者执行对受影响的设备执行命令注入攻击。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR

5. Qualcomm 组件缓冲区错误漏洞（CNNVD-202105-029）

Qualcomm 组件是美国高通（Qualcomm）公司的一个组件。提供高通设备功能的内在部件。

高通组件存在安全漏洞，该漏洞源于解压缩 RTCP 数据包时缓冲区超读，如果 RTCP 数据包中的长度错误，我们可能会读取额外的字节。以下产品及版本受到影响：APQ8009, APQ8009W, APQ8017, APQ8037, APQ8053, APQ8084, APQ8096AU, AQT1000, AR8151, CSR6030, CSRB31024, MDM8207, MDM9150, MDM9205, MDM9206, MDM9207, MDM9250, MDM9607, MDM9625, MDM9628, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8108, MSM8208, MSM8209, MSM8608, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8976SG, MSM8996AU, PM215, PM3003A, PM439, PM456, PM6125, PM6150, PM6150A, PM6150L, PM6250, PM6350, PM640A,

PM640L, PM640P, PM660, PM660A, PM660L, PM670, PM670L, PM7150A, PM7150L, PM7250, PM7250B, PM8004, PM8005, PM8008, PM8009, PM8019, PM8150, PM8150A, PM8150B, PM8150C, PM8150L, PM8250, PM855, PM855A, PM855B, PM855L, PM855P, PM8909, PM8916, PM8937, PM8940, PM8952, PM8953, PM8956, PM8996, PM8998, PMC1000H, PMD9607, PMD9635, PMD9645, PMD9655, PMD9655AU, PME605, PMI632, PMI8937, PMI8940, PMI8952, PMI8994, PMI8996, PMI8998, PMK8001, PMK8002, PMK8003, PMM855AU, PMM8996AU, PMR525, PMR735A, PMR735B, PMW3100, PMX20, PMX24, PMX50, PMX55, QAT3514, QAT3516, QAT3518, QAT3519, QAT3522, QAT3550, QAT3555, QAT5515, QAT5516, QAT5522, QAT5533, QBT1000, QBT1500, QBT2000, QCA4004, QCA4020, QCA6174A, QCA6310, QCA6320, QCA6335, QCA6390, QCA6391, QCA6420, QCA6421, QCA6426, QCA6430, QCA6431, QCA6436, QCA6564A, QCA6564AU, QCA6574, QCA6574A, QCA6574AU, QCA6584, QCA6584AU, QCA6595, QCA6595AU, QCA6694, QCA6694AU, QCA6696, QCA8337, QCA9367, QCA9377, QCA9379, QCC1110, QCM4290, QCM6125, QCS410, QCS4290, QCS603, QCS605, QCS610, QCS6125, QDM2301, QDM2302, QDM2305, QDM2307, QDM2308, QDM2310, QDM3301, QDM5620, QDM5621, QDM5650, QDM5652, QDM5670, QDM5671, QDM5677, QDM5679, QET4100, QET4101, QET4200AQ, QET5100,

QET5100M, QET6100, QET6110, QFE1035, QFE1040, QFE1045, QFE1100, QFE2080FC, QFE2081FC, QFE2082FC, QFE2101, QFE2340, QFE2520, QFE2550, QFE3100, QFE3320, QFE3335, QFE3340, QFE3345, QFE3440FC, QFE4301, QFE4302, QFE4303, QFE4305, QFE4308, QFE4309, QFE4320, QFE4373FC, QFE4455FC, QFE4465FC, QFS2530, QFS2580, QLN1020, QLN1021AQ, QLN1030, QLN1031, QLN1035BD, QLN1036AQ, QLN4640, QLN4642, QLN4650, QLN5020, QLN5030, QLN5040, QPA2625, QPA4340, QPA4360, QPA4361, QPA5373, QPA5460, QPA5580, QPA5581, QPA6560, QPA8673, QPA8675, QPA8686, QPA8801, QPA8802, QPA8803, QPA8821, QPA8842, QPM2630, QPM4650, QPM5620, QPM5621, QPM5657, QPM5658, QPM5670, QPM5677, QPM5679, QPM6582, QPM6585, QPM8820, QPM8830, QPM8870, QPM8895, QSM7250, QSW6310, QSW8573, QSW8574, QTC410S, QTC800H, QTC800S, QTC800T, QTC801S, QTM525, QTM527, Qualcomm215, RGR7640AU, RSW8577, SA415M, SA515M, SA8155, SA8155P, SC8180X+SDX55, SD 455, SD 636, SD 675, SD 8C, SD 8CX, SD205, SD210, SD429, SD439, SD450, SD480, SD632, SD660, SD665, SD670, SD675, SD678, SD690 5G, SD710, SD712, SD720G, SD730, SD750G, SD765, SD765G, SD768G, SD820, SD821, SD835, SD845, SD850, SD855, SD865 5G, SD870, SDM630, SDR051, SDR052, SDR105, SDR660, SDR660G, SDR675, SDR735, SDR735G, SDR8150, SDR8250, SDR845, SDR865,

SDW2500, SDW3100, SDX20, SDX24, SDX50M, SDX55, SDX55M, SDXR1, SDXR2 5G, SM6250, SM6250P, SM7250P, SMB1351, SMB1355, SMB1357, SMB1358, SMB1360, SMB1380, SMB1381, SMB1390, SMB1395, SMB1396, SMB231, SMB2351, SMB358, SMB358S, SMR525, SMR526, WCD9306, WCD9326, WCD9330, WCD9335, WCD9340, WCD9341, WCD9360, WCD9370, WCD9371, WCD9375, WCD9380, WCD9385, WCN3610, WCN3615, WCN3620, WCN3660, WCN3660B, WCN3680, WCN3680B, WCN3910, WCN3950, WCN3980, WCN3988, WCN3990, WCN3991, WCN3998, WCN6850, WCN6851, WCN6855, WCN6856, WFR1620, WGR7640, WHS9410, WSA8810, WSA8815, WSA8830, WSA8835, WTR1625, WTR2955, WTR2965, WTR3905, WTR3925, WTR3950, WTR4605, WTR4905, WTR5975, WTR6955 。

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/may-2021-bulletin

6. Wordpress 基金会 themegrill-demo-importer 访问控制错误漏洞（CNNVD-202105-188）

WordPress 是 Wordpress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress 插件是 WordPress 开源的一个应用插件。

themegrill-demo-importer 1.6.3 之前版本存在安全漏洞，该漏洞源

于清除数据库时不需要身份验证。

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/themegrill/themegrill-demo-importer/commit/564d8496d1f0d10f6aab4798eeec7ddefc81bdd2

7. Microsoft HTTP.sys 资源管理错误漏洞（CNNVD-202105-588）

Microsoft HTTP.sys 是美国微软（Microsoft）公司的一个应用协议。HTTP 应用协议。

HTTP.sys 存在资源管理错误漏洞。以下产品和版本受到影响：Windows 10 Version 2004 for 32-bit Systems,Windows 10 Version 2004 for ARM64-based Systems,Windows 10 Version 2004 for x64-based Systems,Windows Server, version 2004 (Server Core installation),Windows 10 Version 20H2 for x64-based Systems,Windows 10 Version 20H2 for 32-bit Systems,Windows 10 Version 20H2 for ARM64-based Systems,Windows Server, version 20H2 (Server Core Installation)。

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/en-US/security-guidance/advisory/CVE-2021-31166

8. Qualcomm 组件输入验证错误漏洞（CNNVD-202105-031）

Qualcomm 组件是美国高通（Qualcomm）公司的一个组件。提供高通设备功能的内在部件。

高通组件存在输入验证错误漏洞，该漏洞源于不正确的长度检查 SDES 包。以下产品及版本受影响：APQ8009, APQ8009W, APQ8017, APQ8037, APQ8053, APQ8084, APQ8096AU, AQT1000, AR6003, AR8151, CSR6030, CSRB31024, MDM8207, MDM8215, MDM8215M, MDM8615M, MDM9150, MDM9205, MDM9206, MDM9207, MDM9215, MDM9230, MDM9250, MDM9310, MDM9330, MDM9607, MDM9615, MDM9615M, MDM9625, MDM9628, MDM9630, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8108, MSM8208, MSM8209, MSM8608, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8976SG, MSM8996AU, PM215, PM3003A, PM439, PM456, PM6125, PM6150, PM6150A, PM6150L, PM6250, PM640A, PM640L, PM640P, PM660, PM660A, PM660L, PM670, PM670L, PM7150A, PM7150L, PM7250, PM7250B, PM8004, PM8005, PM8008, PM8009, PM8018, PM8019, PM8150, PM8150A, PM8150B, PM8150C, PM8150L, PM8250, PM8350, PM855, PM855A, PM855B, PM855L, PM855P, PM8909, PM8916, PM8937, PM8940, PM8952, PM8953, PM8956, PM8996, PM8998, PMC1000H, PMD9607, PMD9635, PMD9645, PMD9655, PMD9655AU, PME605, PMI632, PMI8937, PMI8940, PMI8952, PMI8994, PMI8996, PMI8998, PMK8001, PMK8002, PMM855AU, PMM8996AU, PMR525, PMR735A, PMW3100, PMX20, PMX24, PMX50, PMX55, QAT3514, QAT3516,

QAT3518, QAT3519, QAT3522, QAT3550, QAT3555, QAT5515, QAT5516, QAT5522, QAT5533, QBT1000, QBT1500, QBT2000, QCA4004, QCA4020, QCA6174, QCA6174A, QCA6234, QCA6310, QCA6320, QCA6335, QCA6390, QCA6391, QCA6420, QCA6421, QCA6426, QCA6430, QCA6431, QCA6436, QCA6564A, QCA6564AU, QCA6574, QCA6574A, QCA6574AU, QCA6584, QCA6584AU, QCA6595, QCA6595AU, QCA6694, QCA6694AU, QCA6696, QCA8337, QCA9367, QCA9377, QCA9379, QCC1110, QCM4290, QCM6125, QCS410, QCS4290, QCS603, QCS605, QCS610, QCS6125, QDM2301, QDM2302, QDM2305, QDM2307, QDM2308, QDM2310, QDM3301, QDM5620, QDM5621, QDM5650, QDM5652, QDM5670, QDM5671, QDM5677, QDM5679, QET4100, QET4101, QET4200AQ, QET5100, QET5100M, QET6110, QFE1035, QFE1040, QFE1045, QFE1100, QFE2080FC, QFE2081FC, QFE2082FC, QFE2101, QFE2340, QFE2520, QFE2550, QFE3100, QFE3320, QFE3335, QFE3340, QFE3345, QFE3440FC, QFE4301, QFE4302, QFE4303, QFE4305, QFE4308, QFE4309, QFE4320, QFE4373FC, QFE4455FC, QFE4465FC, QFS2530, QFS2580, QLN1020, QLN1021AQ, QLN1030, QLN1031, QLN1035BD, QLN1036AQ, QLN4640, QLN4642, QLN4650, QLN5020, QLN5030, QLN5040, QPA2625, QPA4340, QPA4360, QPA4361, QPA5373, QPA5460, QPA5580, QPA6560, QPA8673, QPA8675, QPA8686, QPA8801, QPA8802, QPA8803, QPA8821,

QPA8842, QPM2630, QPM4650, QPM5620, QPM5621, QPM5657, QPM5658, QPM5670, QPM5677, QPM5679, QPM6582, QPM6585, QPM8820, QPM8830, QPM8870, QPM8895, QSM7250, QSW6310, QSW8573, QSW8574, QTC410S, QTC800H, QTC800S, QTC800T, QTC801S, QTM525, QTM527, Qualcomm215, RGR7640AU, RSW8577, SA415M, SA515M, SA8155, SA8155P, SC8180X+SDX55, SD 455, SD 636, SD 675, SD 8C, SD 8CX, SD205, SD210, SD429, SD439, SD450, SD632, SD660, SD665, SD670, SD675, SD678, SD710, SD712, SD720G, SD730, SD765, SD765G, SD768G, SD820, SD821, SD835, SD845, SD850, SD855, SD865 5G, SD870, SD888 5G, SDM630, SDR051, SDR052, SDR105, SDR660, SDR660G, SDR675, SDR735, SDR8150, SDR8250, SDR845, SDR865, SDW2500, SDW3100, SDX20, SDX24, SDX50M, SDX55, SDX55M, SDXR1, SDXR2 5G, SM6250, SM6250P, SM7250P, SMB1350, SMB1351, SMB1355, SMB1357, SMB1358, SMB1360, SMB1380, SMB1381, SMB1390, SMB231, SMB2351, SMB358, SMB358S, SMR525, SMR526, SMR545, SMR546, WCD9306, WCD9326, WCD9330, WCD9335, WCD9340, WCD9341, WCD9360, WCD9370, WCD9371, WCD9375, WCD9380, WCD9385, WCN3610, WCN3615, WCN3620, WCN3660, WCN3660B, WCN3680, WCN3680B, WCN3910, WCN3950, WCN3980, WCN3988, WCN3990, WCN3991, WCN3998, WCN6850, WCN6851, WCN6855, WCN6856, WFR1620, WGR7640, WHS9410, WSA8810, WSA8815, WTR1605,

WTR1605L, WTR1625, WTR2955, WTR2965, WTR3905, WTR3925, WTR3950, WTR4605, WTR4905, WTR5975, WTR6955 。

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/may-2021-bulletin

1.4.2 高危漏洞实例

本月高危漏洞共 617 个，其中重点漏洞实例如表 6 所示。

表 6　2021 年 5 月高危漏洞实例

序号	漏洞类型	厂商	CNNVD 编号	漏洞实例
1	SQL 注入	Cisco	CNNVD-202105-237	思科 Cisco Unified Communications Manager SQL 注入漏洞（CNNVD-202105-236）
			CNNVD-202105-236	
		Hexagon	CNNVD-202105-653	
		IBM	CNNVD-202105-1404	
		Liferay	CNNVD-202105-806	
		OpenEMR 社区	CNNVD-202105-355	
			CNNVD-202105-334	
		Progress Software	CNNVD-202105-1223	
		WordPress 基金会	CNNVD-202105-1299	
		Wordpress 基金会	CNNVD-202105-1148	
		个人开发者	CNNVD-202105-1508	
2	代码问题	3S-Smart Software Solutions	CNNVD-202105-051	Rockwell Automation Connected Components Workbench 代码问题漏洞（CNNVD-202105-805）
		Admidio	CNNVD-202105-1324	
		Antisip	CNNVD-202105-781	
		Bitdefender	CNNVD-202105-1225	
		Cisco	CNNVD-202105-214	
			CNNVD-202105-218	
			CNNVD-202105-217	
			CNNVD-202105-152	
			CNNVD-202105-215	
			CNNVD-202105-216	

			CNNVD-202105-219	
		Django 基金会	CNNVD-202105-092	
		Elasticsearch	CNNVD-202105-288	
		FFmpeg 团队	CNNVD-202105-1649	
		Google	CNNVD-202105-957	
			CNNVD-202105-880	
			CNNVD-202105-901	
			CNNVD-202105-888	
			CNNVD-202105-902	
			CNNVD-202105-951	
			CNNVD-202105-941	
			CNNVD-202105-875	
			CNNVD-202105-997	
			CNNVD-202105-871	
		IBM	CNNVD-202105-064	
		Jenkins	CNNVD-202105-559	
			CNNVD-202105-1591	
		JetBrains	CNNVD-202105-685	
			CNNVD-202105-665	
		Linux 基金会	CNNVD-202105-1661	
		MOXA	CNNVD-202105-510	
		Overwolf	CNNVD-202105-1348	
		Rockwell Automation	CNNVD-202105-805	
		Teradici	CNNVD-202105-846	
			CNNVD-202105-819	
		Ubiquiti	CNNVD-202105-1194	
		Windscribe	CNNVD-202105-501	
		Wordpress 基金会	CNNVD-202105-261	
			CNNVD-202105-991	
			CNNVD-202105-262	
			CNNVD-202105-263	
			CNNVD-202105-257	
		个人开发者	CNNVD-202105-1388	
			CNNVD-202105-1384	
			CNNVD-202105-352	
			CNNVD-202105-1196	
			CNNVD-202105-1192	
			CNNVD-202105-1398	
3	授权问题	Apache 基金会	CNNVD-202105-1589	Red Hat OpenShift GitOps 授权问题漏洞（CNNVD-202105-1288）
		Atlassian	CNNVD-202105-476	
		Commscope	CNNVD-202105-1785	
		Dell	CNNVD-202105-124	

		IBM	CNNVD-202105-982	
		JetBrains	CNNVD-202105-688	
		Liferay	CNNVD-202105-609	
		PAX	CNNVD-202105-341	
		Red Hat	CNNVD-202105-1288	
		Trend Micro	CNNVD-202105-298	
		Versa Networks	CNNVD-202105-1714	
		WordPress 基金会	CNNVD-202105-980	
		Wordpress 基金会	CNNVD-202105-987	
			CNNVD-202105-979	
			CNNVD-202105-983	
			CNNVD-202105-984	
			CNNVD-202105-981	
			CNNVD-202105-985	
			CNNVD-202105-986	
		个人开发者	CNNVD-202105-727	
			CNNVD-202105-273	
			CNNVD-202105-792	
4	操作系统命令注入	Adobe	CNNVD-202105-716	Adobe After Effects 操作系统命令注入漏洞（CNNVD-202105-716）
		Cisco	CNNVD-202105-141	
			CNNVD-202105-1279	
			CNNVD-202105-209	
			CNNVD-202105-1297	
			CNNVD-202105-1298	
		EyesOfNetwork 社区	CNNVD-202105-1513	
		Hongdian	CNNVD-202105-281	
		IBM	CNNVD-202105-1402	
		Pulse Secure	CNNVD-202105-190	
		Sonicwall	CNNVD-202105-1820	
		个人开发者	CNNVD-202105-125	
5	缓冲区错误	3S-Smart Software Solutions	CNNVD-202105-1627	Microsoft Internet Explorer 缓冲区错误漏洞（CNNVD-202105-587）
			CNNVD-202105-1620	
		Adobe	CNNVD-202105-603	
			CNNVD-202105-741	
			CNNVD-202105-598	
			CNNVD-202105-601	
			CNNVD-202105-748	
			CNNVD-202105-736	
			CNNVD-202105-749	

			CNNVD-202105-738	
			CNNVD-202105-606	
			CNNVD-202105-742	
			CNNVD-202105-740	
		Apple	CNNVD-202105-1564	
			CNNVD-202105-060	
			CNNVD-202105-1448	
			CNNVD-202105-1526	
			CNNVD-202105-1446	
			CNNVD-202105-1567	
			CNNVD-202105-1568	
			CNNVD-202105-1558	
			CNNVD-202105-1569	
			CNNVD-202105-1574	
			CNNVD-202105-1566	
			CNNVD-202105-004	
			CNNVD-202105-1534	
			CNNVD-202105-1532	
			CNNVD-202105-1450	
			CNNVD-202105-1573	
			CNNVD-202105-1533	
			CNNVD-202105-1544	
		Arch	CNNVD-202105-1684	
		Cisco	CNNVD-202105-227	
			CNNVD-202105-228	
		Delta Electronics	CNNVD-202105-090	
		Epic Games	CNNVD-202105-1214	
		FFmpeg 团队	CNNVD-202105-1497	
			CNNVD-202105-1819	
		Foxit	CNNVD-202105-707	
			CNNVD-202105-309	
			CNNVD-202105-320	
			CNNVD-202105-371	
			CNNVD-202105-378	
			CNNVD-202105-368	
			CNNVD-202105-313	
		GNU 社区	CNNVD-202105-1193	
			CNNVD-202105-1190	
			CNNVD-202105-1117	
			CNNVD-202105-1191	
			CNNVD-202105-1106	
			CNNVD-202105-1124	

			CNNVD-202105-1114	
			CNNVD-202105-1125	
			CNNVD-202105-1110	
			CNNVD-202105-1113	
			CNNVD-202105-1105	
			CNNVD-202105-1134	
			CNNVD-202105-1185	
			CNNVD-202105-1111	
			CNNVD-202105-1104	
			CNNVD-202105-1127	
		Google	CNNVD-202105-519	
			CNNVD-202105-1594	
			CNNVD-202105-1001	
			CNNVD-202105-071	
			CNNVD-202105-1002	
			CNNVD-202105-894	
			CNNVD-202105-886	
			CNNVD-202105-936	
			CNNVD-202105-903	
			CNNVD-202105-918	
			CNNVD-202105-881	
			CNNVD-202105-937	
			CNNVD-202105-1010	
			CNNVD-202105-913	
			CNNVD-202105-911	
			CNNVD-202105-027	
			CNNVD-202105-1004	
			CNNVD-202105-916	
			CNNVD-202105-1012	
			CNNVD-202105-956	
			CNNVD-202105-909	
			CNNVD-202105-1005	
			CNNVD-202105-908	
			CNNVD-202105-1011	
			CNNVD-202105-962	
			CNNVD-202105-1003	
			CNNVD-202105-905	
			CNNVD-202105-934	
		HP	CNNVD-202105-1312	
		Hilscher	CNNVD-202105-822	
		IBM	CNNVD-202105-289	
		Linux 基金会	CNNVD-202105-1772	
			CNNVD-202105-271	

			CNNVD-202105-1645	
		Microsoft	CNNVD-202105-587	
		Omron	CNNVD-202105-706	
		Pulse Secure	CNNVD-202105-191	
		Qualcomm	CNNVD-202105-030	
			CNNVD-202105-028	
		Siemens	CNNVD-202105-477	
			CNNVD-202105-636	
			CNNVD-202105-542	
			CNNVD-202105-550	
			CNNVD-202105-1957	
			CNNVD-202105-764	
			CNNVD-202105-769	
		个人开发者	CNNVD-202105-112	
			CNNVD-202105-1189	
			CNNVD-202105-524	
			CNNVD-202105-1205	
			CNNVD-202105-234	
			CNNVD-202105-1750	
			CNNVD-202105-1997	
			CNNVD-202105-1791	
			CNNVD-202105-116	
			CNNVD-202105-104	
			CNNVD-202105-094	
			CNNVD-202105-109	
			CNNVD-202105-113	
			CNNVD-202105-869	
			CNNVD-202105-1206	
6	访问控制错误	Autodesk	CNNVD-202105-1950	Siemens SINAMICS SL150 访问控制错误漏洞（CNNVD-202105-628）
		Cisco	CNNVD-202105-146	
		Qnap Systems	CNNVD-202105-813	
		Red Hat	CNNVD-202105-1715	
		STMicroelectronics	CNNVD-202105-1364	
		Siemens	CNNVD-202105-628	
		个人开发者	CNNVD-202105-1949	
7	资源管理错误	Adobe	CNNVD-202105-597	Microsoft Excel 资源管理错误漏洞（CNNVD-202105-594）
			CNNVD-202105-612	
			CNNVD-202105-618	
			CNNVD-202105-737	
		Apple	CNNVD-202105-1577	
			CNNVD-202105-1522	
		Cisco	CNNVD-202105-220	

		Foxit	CNNVD-202105-356	
			CNNVD-202105-363	
			CNNVD-202105-369	
			CNNVD-202105-312	
			CNNVD-202105-319	
			CNNVD-202105-246	
			CNNVD-202105-325	
			CNNVD-202105-353	
			CNNVD-202105-331	
			CNNVD-202105-340	
			CNNVD-202105-304	
			CNNVD-202105-311	
			CNNVD-202105-315	
		Google	CNNVD-202105-499	
			CNNVD-202105-1590	
			CNNVD-202105-1593	
			CNNVD-202105-511	
			CNNVD-202105-1596	
			CNNVD-202105-1611	
			CNNVD-202105-1592	
			CNNVD-202105-072	
			CNNVD-202105-509	
			CNNVD-202105-1603	
		HAXX	CNNVD-202105-1683	
		JetBrains	CNNVD-202105-666	
		Linux 基金会	CNNVD-202105-865	
			CNNVD-202105-760	
			CNNVD-202105-714	
		Microsoft	CNNVD-202105-595	
			CNNVD-202105-596	
			CNNVD-202105-594	
		Mozilla 基金会	CNNVD-202105-056	
		Prosodical Thoughts	CNNVD-202105-838	
			CNNVD-202105-840	
		Qualcomm	CNNVD-202105-008	
			CNNVD-202105-009	
			CNNVD-202105-025	
			CNNVD-202105-005	
		Schneider Electric	CNNVD-202105-1725	
		Siemens	CNNVD-202105-615	
			CNNVD-202105-575	
		Stormshield	CNNVD-202105-133	

		个人开发者	CNNVD-202105-701	
			CNNVD-202105-238	
			CNNVD-202105-1381	
			CNNVD-202105-1666	
			CNNVD-202105-121	
			CNNVD-202105-963	
			CNNVD-202105-278	
			CNNVD-202105-1013	
8	输入验证错误	3S-Smart Software Solutions	CNNVD-202105-050	Vmware vSphere Client 输入验证错误漏洞（CNNVD-202105-1686）
		Adobe	CNNVD-202105-750	
		Apple	CNNVD-202105-061	
		Cisco	CNNVD-202105-223	
			CNNVD-202105-143	
			CNNVD-202105-222	
			CNNVD-202105-224	
		Google	CNNVD-202105-884	
		Linux 基金会	CNNVD-202105-1644	
		Nagios	CNNVD-202105-1479	
		Qualcomm	CNNVD-202105-040	
			CNNVD-202105-024	
			CNNVD-202105-038	
		Redis Labs	CNNVD-202105-103	
			CNNVD-202105-105	
		Rockwell Automation	CNNVD-202105-802	
		Vmware	CNNVD-202105-1686	
		ZOHO	CNNVD-202105-818	
		个人开发者	CNNVD-202105-1182	
			CNNVD-202105-498	
			CNNVD-202105-110	

1. 思科 Cisco Unified Communications Manager SQL 注入漏洞（CNNVD-202105-236）

Cisco Unified Communications Manager（CUCM，Unified CM，CallManager）是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。该组件提供了一种可扩展、可分布和高可用的企业 IP 电话呼叫处理解决方案。

Cisco Unified Communications Manager IM & 的 web 管理界面存在 SQL 注入漏洞，该漏洞源于用户提交的参数验证不当造成的。攻击者可利用该漏洞通过对应用程序进行身份验证并向受影响的系统发送恶意请求。

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-imp-inj-ereCOKjR

2. Rockwell Automation Connected Components Workbench 代码问题漏洞（CNNVD-202105-805）

Rockwell Automation Connected Components Workbench 是美国罗克韦尔（Rockwell Automation ）公司的一个应用软件。一个自动编程软件。

Connected Components Workbench 12.00.00 版本及之前存在代码问题漏洞。该漏洞源于程序的组件工作台不限制可以反序列化的对象，攻击者可以利用该漏洞远程执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1131435

3. Red Hat OpenShift GitOps 授权问题漏洞（CNNVD-202105-1288）

Red Hat OpenShift 是美国红帽（Red Hat）公司的一款平台即服务（PaaS）云计算平台，它支持构建、测试、部署和运行应用程序。

Red Hat OpenShift GitOps 存在安全漏洞，该漏洞源于 argocd：ServiceAccount argocd-argocd-server 能够读取整个集群的所有资源。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://access.redhat.com/errata/RHSA-2021:2053

4. Adobe After Effects 操作系统命令注入漏洞（CNNVD-202105-716）

Adobe After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。

Adobe After Effects 存在操作系统命令注入漏洞。该漏洞源于程序输入验证不正确导致，远程未经身份验证的攻击者可以将特制数据传递到应用程序并在目标系统上执行任意 OS 命令。以下产品及版本受到影响：Adobe After Effects： 17.0.0、17.0.1、17.0.3、17.0.6、17.1、17.1.1、17.1.3、18.0、18.1。

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/after_effects/apsb21-33.html

5. Microsoft Internet Explorer 缓冲区错误漏洞（CNNVD-202105-587）

Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。

Internet Explorer 存在缓冲区错误漏洞。以下产品和版本受到影

响：Internet Explorer 11,Internet Explorer 9。

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/en-US/security-guidance/advisory/CVE-2021-26419

6. Siemens SINAMICS SL150 访问控制错误漏洞（CNNVD-202105-628）

Siemens SINAMICS SL150 是德国西门子（Siemens）公司的一个应用程序。用于高转矩慢速同步和感应电动机的循环变频器。

多款 Siemens 设备存在访问控制错误漏洞。该漏洞源于系统组件的 Telnet 服务不需要身份验证，如果启用了该服务，则它可能允许远程攻击者访问设备。以下产品及版本受到影响：SINAMICS SL150、SINAMICS SM150、SINAMICS SM150i。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://cert-portal.siemens.com/productcert/pdf/ssa-752103.pdf

7. Microsoft Excel 资源管理错误漏洞（CNNVD-202105-594）

Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。

Microsoft Office Excel 存在资源管理错误漏洞。以下产品和版本受到影响：Microsoft Office 2019 for 32-bit editions,Microsoft Office 2019 for 64-bit editions,Microsoft Office 2019 for Mac,Microsoft Office Online Server,Microsoft 365 Apps for Enterprise for 32-bit Systems,Microsoft 365 Apps for Enterprise for 64-bit Systems,Microsoft

Excel 2016 (32-bit edition),Microsoft Excel 2016 (64-bit edition),Microsoft Excel 2013 RT Service Pack 1,Microsoft Excel 2013 Service Pack 1 (32-bit editions),Microsoft Excel 2013 Service Pack 1 (64-bit editions),Microsoft Office Web Apps Server 2013 Service Pack 1。

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/en-US/security-guidance/advisory/CVE-2021-31177

8. Vmware vSphere Client 输入验证错误漏洞（CNNVD-202105-1686）

Vmware vSphere Client 是美国威睿（Vmware）公司的一个应用软件。提供虚拟化管理。

vSphere Client 存在安全漏洞，该漏洞由于 vCenter Server 默认启用的虚拟 SAN 健康检查插件缺乏输入验证导致底层操作系统上以不受限制的权限执行命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.vmware.com/security/advisories/VMSA-2021-0010.html

二、接报漏洞情况

本月接报漏洞 5806 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）5521 个。

表 7 2021 年 5 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	2766
2	上海斗象信息科技有限公司	1353
3	河南听潮盛世信息技术有限公司	320
4	北京山石网科信息技术有限公司	263
5	长春嘉诚信息技术股份有限公司	181
6	内蒙古奥创科技有限公司	159
7	北京天地和兴科技有限公司	88
8	南京众智维信息科技有限公司	84
9	北京数字观星科技有限公司	72
10	北京鸿腾智能科技有限公司	55
11	西安四叶草信息技术有限公司	43
12	北京安帝科技有限公司	38
13	深信服科技股份有限公司	26
14	山东云天安全技术有限公司	25
15	广州锦行网络科技有限公司	20
16	星云博创摘星实验室	20
17	北京天融信网络安全技术有限公司	19
18	上海上讯信息技术股份有限公司	18
19	北京顶象技术有限公司 洞见安全实验室	16
20	北京圣博润高新技术股份有限公司	15
21	中兴通讯	15
22	广州易东信息安全技术有限公司	14
23	中国电信集团系统集成有限责任公司	14

24	北京华云安信息技术有限公司	13
25	北京墨云科技有限公司	13
26	北京梆梆安全科技有限公司	10
27	内蒙古中叶信息技术有限责任公司	10
28	山东新潮信息技术有限公司	10
29	江苏金盾检测技术有限公司	9
30	广州竞远安全技术股份有限公司	8
31	华为技术有限公司未然实验室	8
32	清华大学	8
33	安全邦（北京）信息技术有限公司	7
34	北京市星阑科技有限公司	7
35	杭州安恒信息	6
36	杭州安恒信息技术股份有限公司	6
37	上海天民信息技术有限公司	6
38	个人	5
39	北京江南天安科技有限公司	5
40	恒安嘉新（北京）科技股份公司	5
41	浪潮电子信息产业股份有限公司	5
42	北京启明星辰信息安全技术有限公司	4
43	海南神州希望网络有限公司	4
44	内蒙古思沃科技有限公司	4
45	阿里集团安全部	3
46	博智安全科技股份有限公司	2

47	上海上讯信息技术股份有限公司	2
48	国防科技大学	2
49	绿盟科技集团股份有限公司	2
50	四川大学网络空间安全学院	2
51	中孚安全技术有限公司	2
52	中通服咨询设计研究院有限公司	2
53	北京信联科汇科技有限公司	1
54	北京云测信息科技有限公司	1
55	北京智游网安科技有限公司	1
56	博智安全科技股份有限公司	1
57	太平金融科技服务（上海）有限公司	1
58	中测安华科技有限公司	1
59	中资网络信息安全科技有限公司	1
60	重庆梦之想科技有限责任公司	1
报送总计		5806

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 Visual Studio 代码注入漏洞（CNNVD-202105-625、CVE-2021-27068）、Microsoft Windows Codecs 代码注入漏洞（CNNVD-202105-646、CVE-2021-28465）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。

.漏洞介绍

2021 年 5 月 12 日，微软发布了 2021 年 5 月份安全更新，共 55 个漏洞的补丁程序，CNNVD 对这些漏洞进行了收录。本次更新主要涵盖了 Windows 操作系统、Exchange Server、.Net、Office、SharePoint、Hyper-V、Visual Studio 等。CNNVD 对其危害等级进行了评价，其中高危漏洞有 19 个，中危漏洞 34 个，低危漏洞 2 个。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

此次更新共包括 55 个漏洞的补丁程序，其中高危漏洞有 19 个，中危漏洞 34 个，低危漏洞 2 个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	官方链接
1	Microsoft Visual Studio 代码注入漏洞	CNNVD-202105-625	CVE-2021-27068	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27068
2	Microsoft Jet Database Engine 代码注入漏洞	CNNVD-202105-599	CVE-2021-28455	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28455
3	Microsoft Windows Codecs 代码注入漏洞	CNNVD-202105-646	CVE-2021-28465	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28465

4	Microsoft Office SharePoint 代码注入漏洞	CNNVD-202105-556	CVE-2021-28474	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28474
5	Microsoft Hyper-V 代码注入漏洞	CNNVD-202105-586	CVE-2021-28476	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476
6	Microsoft HTTP.sys 代码注入漏洞	CNNVD-202105-588	CVE-2021-31166	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166
7	Microsoft Office Excel 代码注入漏洞	CNNVD-202105-596	CVE-2021-31175	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31175
8	Microsoft Office 代码注入漏洞	CNNVD-202105-595	CVE-2021-31176	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31176
9	Microsoft Office Excel 代码注入漏洞	CNNVD-202105-594	CVE-2021-31177	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31177
10	Microsoft Office Excel 代码注入漏洞	CNNVD-202105-593	CVE-2021-31179	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31179
11	Microsoft Office Word 代码注入漏洞	CNNVD-202105-592	CVE-2021-31180	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31180
12	Microsoft SharePoint 代码注入漏洞	CNNVD-202105-549	CVE-2021-31181	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31181
13	Microsoft Windows Codecs 代码注入漏洞	CNNVD-202105-570	CVE-2021-31192	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31192
14	Microsoft OLE Automation Remote code 代码注入漏洞	CNNVD-202105-569	CVE-2021-31194	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31194
15	Microsoft Exchange Server 代码注入漏洞	CNNVD-202105-551	CVE-2021-31195	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31195
16	Microsoft Exchange Server 代码注入漏洞	CNNVD-202105-547	CVE-2021-31198	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31198

17	Microsoft Visual Studio Code 代码注入漏洞	CNNVD-202105-700	CVE-2021-31211	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31211
18	Microsoft Visual Studio Code 代码注入漏洞	CNNVD-202105-677	CVE-2021-31213	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31213
19	Microsoft Visual Studio Code 代码注入漏洞	CNNVD-202105-696	CVE-2021-31214	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31214
20	Microsoft Windows Wireless Networking 信息泄露漏洞	CNNVD-202105-632	CVE-2020-24587	中危	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00473.html
21	Microsoft Windows Wireless Networking 安全漏洞	CNNVD-202105-633	CVE-2020-24588	中危	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00473.html
22	Microsoft Windows Wireless Networking 安全漏洞	CNNVD-202105-635	CVE-2020-26144	中危	https://www.wi-fi.org/security-update-fragmentation
23	Microsoft Office SharePoint 安全漏洞	CNNVD-202105-557	CVE-2021-26418	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26418
24	Microsoft Internet Explorer 缓冲区错误漏洞	CNNVD-202105-587	CVE-2021-26419	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26419
25	Microsoft Skype for Business Server 安全漏洞	CNNVD-202105-623	CVE-2021-26421	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26421
26	Microsoft Skype for Business Server 代码注入漏洞	CNNVD-202105-619	CVE-2021-26422	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26422
27	Microsoft Dynamics Finance & Operations 跨站脚本漏洞	CNNVD-202105-638	CVE-2021-28461	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28461

28	Microsoft SharePoint 安全漏洞	CNNVD-202105-555	CVE-2021-28478	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28478
29	Microsoft Windows CSC Service 信息泄露漏洞	CNNVD-202105-589	CVE-2021-28479	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28479
30	Microsoft Windows Container Manager Service 权限许可和访问控制问题漏洞	CNNVD-202105-584	CVE-2021-31165	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31165
31	Microsoft Windows Container Manager Service 权限许可和访问控制问题漏洞	CNNVD-202105-585	CVE-2021-31167	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31167
32	Microsoft Windows Container Manager Service 权限许可和访问控制问题漏洞	CNNVD-202105-583	CVE-2021-31168	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31168
33	Microsoft Windows Container Manager Service 权限许可和访问控制问题漏洞	CNNVD-202105-582	CVE-2021-31169	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31169
34	Microsoft Graphics Components 权限许可和访问控制问题漏洞	CNNVD-202105-581	CVE-2021-31170	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31170
35	Microsoft SharePoint 安全漏洞	CNNVD-202105-553	CVE-2021-31172	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31172
36	Microsoft SharePoint 信息泄露漏洞	CNNVD-202105-552	CVE-2021-31173	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31173

37	Microsoft Excel 信息泄露漏洞	CNNVD-202105-600	CVE-2021-31174	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31174
38	Microsoft Office Excel 信息泄露漏洞	CNNVD-202105-591	CVE-2021-31178	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31178
39	Microsoft Bluetooth Driver 安全漏洞	CNNVD-202105-580	CVE-2021-31182	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31182
40	Microsoft Windows IrDA 缓冲区错误漏洞	CNNVD-202105-579	CVE-2021-31184	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31184
41	Microsoft Windows Desktop Bridge 输入验证错误漏洞	CNNVD-202105-578	CVE-2021-31185	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31185
42	Microsoft Remote Desktop Protocol 信息泄露漏洞	CNNVD-202105-577	CVE-2021-31186	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31186
43	Microsoft Windows WalletService 权限许可和访问控制问题漏洞	CNNVD-202105-576	CVE-2021-31187	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31187
44	Microsoft Graphics Components 权限许可和访问控制问题漏洞	CNNVD-202105-574	CVE-2021-31188	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31188
45	Microsoft Windows Container Isolation FS Filter Driver 权限许可和访问控制问题漏洞	CNNVD-202105-573	CVE-2021-31190	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31190
46	Microsoft Projected File System 缓冲区错误漏洞	CNNVD-202105-572	CVE-2021-31191	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31191

47	Microsoft Windows SSDP Service 权限许可和访问控制问题漏洞	CNNVD-202105-568	CVE-2021-31193	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31193
48	Microsoft Common Utilities 代码注入漏洞	CNNVD-202105-645	CVE-2021-31200	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31200
49	Microsoft Visual Studio 权限许可和访问控制问题漏洞	CNNVD-202105-624	CVE-2021-31204	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31204
50	Microsoft Exchange Server 安全特征问题漏洞	CNNVD-202105-543	CVE-2021-31207	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207
51	Microsoft Windows Container Manager Service 权限许可和访问控制问题漏洞	CNNVD-202105-566	CVE-2021-31208	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31208
52	Microsoft Exchange Server 安全漏洞	CNNVD-202105-544	CVE-2021-31209	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31209
53	Microsoft Accessibility Insights for Web 信息泄露漏洞	CNNVD-202105-644	CVE-2021-31936	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31936
54	Microsoft SharePoint 信息泄露漏洞	CNNVD-202105-554	CVE-2021-31171	低危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31171
55	Microsoft Windows SMB Client 安全特征问题漏洞	CNNVD-202105-567	CVE-2021-31205	低危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31205

.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。微软官方补丁下载地址：

https://msrc.microsoft.com/update-guide/en-us

3.2 Microsoft HTTP.sys 代码注入漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Microsoft HTTP.sys 代码注入漏洞（CNNVD-202105-588、CVE-2021-31166）情况的报送。未授权的攻击者可以构造恶意请求包攻击目标服务器，从而在目标服务器执行任意代码。Windows Server 和 Windows 10 多个版本均受此漏洞影响。目前，微软官方已发布漏洞补丁修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

.漏洞介绍

Microsoft HTTP.sys 是美国微软（Microsoft）公司的一个应用协议。该漏洞存在于 Windows 10 和 Windows Server 中的 HTTP 协议栈(http.sys)处理程序中。未授权的攻击者可以构造恶意请求包攻击目标服务器，从而在目标服务器执行任意代码。

目前，漏洞利用代码已在网络中公布，该漏洞在微软 5 月补丁日中完成了修复，微软官方将其标记为可造成蠕虫攻击及易被攻击的漏洞。

.危害影响

未授权的攻击者可以构造恶意请求包攻击目标服务器，从而在目标服务器执行任意代码。Windows Server, version 20H2、Windows Server, version 2004、Windows 10 Version 20H2 for ARM64-based Systems、Windows 10 Version 20H2 for 32-bit Systems、Windows

10 Version 20H2 for x64-based Systems、Windows 10 Version 2004 for x64-based Systems、Windows 10 Version 2004 for ARM64-based Systems、Windows 10 Version 2004 for 32-bit Systems 等多个版本均受此漏洞影响。

.修复建议

目前，微软官方已发布漏洞补丁修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31166