北京师范大学网络信息安全通告

2022 年 5 月报告

北京师范大学信息网络中心

2022 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，2022 年 5 月份新增安全漏洞共 2044 个，从厂商分布来看，WordPress 基金会公司产品的漏洞数量最多，共发布 146 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 12.67%。本月新增漏洞中，超危漏洞 359 个、高危漏洞 734 个、中危漏洞 862 个、低危漏洞 89 个，相应修复率分别为 53.48%、80.65%、85.27%以及 92.13%。合计 1601 个漏洞已有修复补丁发布，本月整体修复率 78.33%。

截至 2022 年 5 月 31 日，CNNVD 采集漏洞总量已达 184784 个。

1.1 漏洞增长概况

2022 年 4 月新增安全漏洞 2098 个，与上月（2065 个）相比增加了 1.60%。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 1939 个。

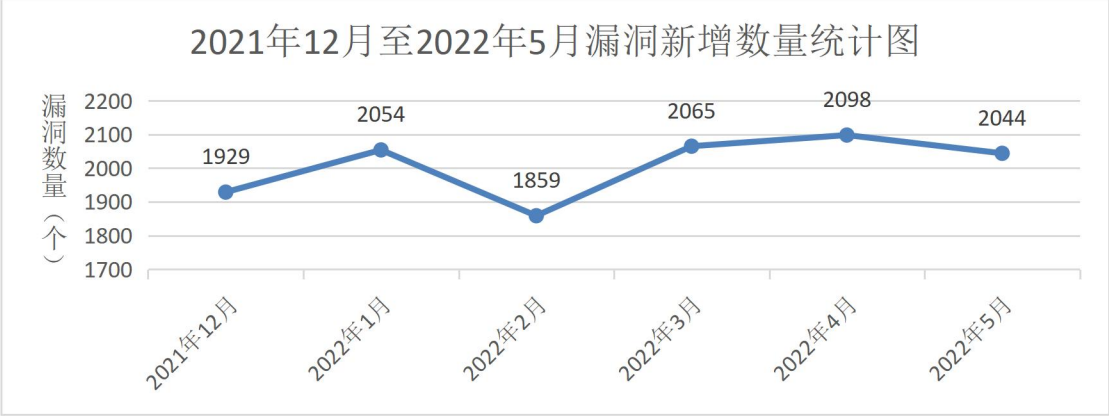

图 1 2021 年 12 月至 2022 年 5 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2022 年 5 月厂商漏洞数量分布情况如表 1 所示，WordPress 基金会公司漏洞达到 146 个，占本月漏洞总量的 7.14%。

表 1　2022 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	WordPress 基金会	146	7.14%
2	Google	83	4.06%
3	Apple	79	3.86%
4	Microsoft	78	3.82%
5	F5	44	2.15%
6	Intel	38	1.86%
7	IBM	36	1.76%
8	AMD	34	1.66%
9	Siemens	30	1.47%
10	Mozilla 基金会	29	1.42%

1.2.2 漏洞产品分布

2022 年 5 月主流操作系统的漏洞统计情况如表 2 所示。本月 Windows 系列操作系统漏洞数量共 65 个[1]，Windows Server 2022 漏洞数量最多，共 58 个，占主流操作系统漏洞总量的 10.55%，排名第一。

表 2　2022 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 Server 2022	58
2	Windows Server 2019	58
3	Windows Server 2016	53
4	Windows 10	46
5	Windows 11	46

[1] Windows 系列操作系统多个版本可能同时受同一个漏洞影响。

6	Windows Server 2012	46
7	Windows Server 2012 R2	46
8	Windows 8.1	36
9	Windows Rt 8.1	36
10	Windows Server 2008	30
11	Windows Server 2008 R2	30
12	Windows 7	29
13	Android	21
14	Linux Kernel	15

1.2.3 漏洞类型分布

2022 年 5 月份发布的漏洞类型分布如表 3 所示，其中跨站脚本类漏洞所占比例最大，约为 12.67%。

表 3 2022 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	跨站脚本	259	12.67%
2	缓冲区错误	195	9.54%
3	SQL 注入	193	9.44%
4	输入验证错误	140	6.85%
5	代码问题	127	6.21%
6	资源管理错误	85	4.16%
7	命令注入	58	2.84%
8	信息泄露	56	2.74%
9	授权问题	46	2.25%
10	访问控制错误	43	2.10%
11	权限许可和访问控制问题	40	1.96%
12	路径遍历	34	1.66%
13	操作系统命令注入	34	1.66%
14	安全特征问题	28	1.37%
15	竞争条件问题	27	1.32%
16	跨站请求伪造	26	1.27%
17	信任管理问题	16	0.78%
18	代码注入	15	0.73%
19	加密问题	13	0.64%
20	注入	6	0.29%
21	数据伪造问题	6	0.29%
22	后置链接	6	0.29%

23	参数注入	5	0.24%
24	日志信息泄露	4	0.20%
25	数字错误	4	0.20%
26	其他	578	28.28%

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。2022 年 5 月漏洞危害等级分布如图 2 所示，其中超危漏洞 359 条，占本月漏洞总数的 17.56%。

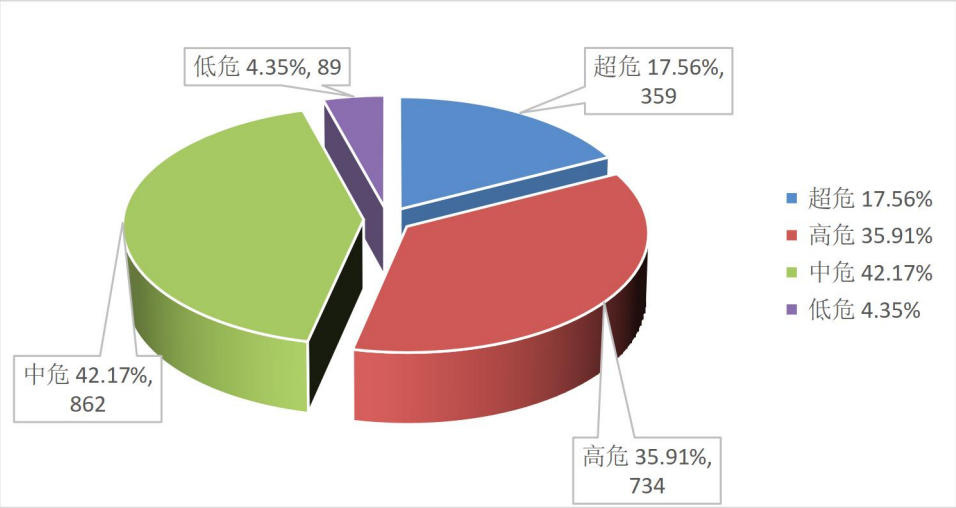

图 2　2022 年 5 月漏洞危害等级分布

1.3 漏洞修复情

1.3.1 整体修复情况

2022 年 5 月漏洞修复情况按危害等级进行统计见图 3。其中低危漏洞修复率最高，达到 92.13%，超危漏洞修复率最低，比例为 53.48%。

总体来看，本月整体修复率，由上月的 77.26%上升至本月的 78.33%。

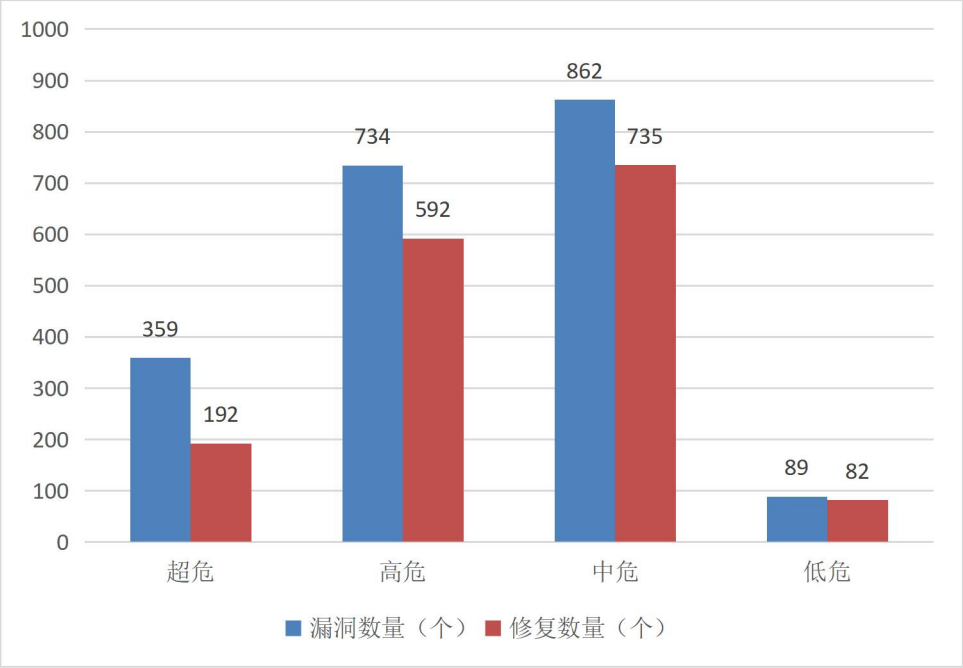

图 3　2022 年 5 月漏洞修复数量统计

1.3.2 厂商修复情况

2022 年 5 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 WordPress 基金会、Google、Apple 等十个厂商共 597 条漏洞，占本月漏洞总数的 29.21%，漏洞修复率为 95.48%，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、Apple、Microsoft、Intel、IBM、AMD、Siemens、Mozilla 基金会等公司本月漏洞修复率均为 100%，共 570 条漏洞已全部修复。

表 4　2022 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	WordPress 基金会	146	120	82.19%
2	Google	83	83	100.00%
3	Apple	79	79	100.00%

4	Microsoft	78	78	100.00%
5	F5	44	43	97.73%
6	Intel	38	38	100.00%
7	IBM	36	36	100.00%
8	AMD	34	34	100.00%
9	Siemens	30	30	100.00%
10	Mozilla 基金会	29	29	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

2022 年 5 月超危漏洞共 359 个，其中重要漏洞实例如表 5 所示。

表 5　2022 年 5 月超危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例
SQL注入	Allgeier Inovar	CNNVD-202205-3515	OpenLDAP SQL注入漏洞（CNNVD-202205-2146）
	Broadcom	CNNVD-202205-2587	
	Cambium Networks	CNNVD-202205-3057	
	Enhancesoft	CNNVD-202205-2136	
	Explore IT	CNNVD-202205-2720	
	IBM	CNNVD-202205-3170	
	MingSoft	CNNVD-202205-1881	
	NETGEAR	CNNVD-202205-3298	
	OpenMRS	CNNVD-202205-2795	
	Openldap基金会	CNNVD-202205-2146	
	Wealth Management System	CNNVD-202205-2712	
	WordPress基金会	CNNVD-202205-1888	
		CNNVD-202205-1892	
		CNNVD-202205-1893	
		CNNVD-202205-1894	
		CNNVD-202205-2698	
		CNNVD-202205-2701	
		CNNVD-202205-2703	
		CNNVD-202205-2705	
		CNNVD-202205-2706	
		CNNVD-202205-2708	
		CNNVD-202205-2709	
		CNNVD-202205-3471	
		CNNVD-202205-3949	

		CNNVD-202205-3951
	Wuzhi	CNNVD-202205-2082
	ZOHO	CNNVD-202205-2521
	wdja团队	CNNVD-202205-2093
	个人开发者	CNNVD-202205-1957
		CNNVD-202205-1971
		CNNVD-202205-1972
		CNNVD-202205-2083
		CNNVD-202205-2091
		CNNVD-202205-2100
		CNNVD-202205-2467
		CNNVD-202205-2490
		CNNVD-202205-2493
		CNNVD-202205-2577
		CNNVD-202205-2793
		CNNVD-202205-2926
		CNNVD-202205-2928
		CNNVD-202205-2929
		CNNVD-202205-2942
		CNNVD-202205-2944
		CNNVD-202205-2947
		CNNVD-202205-2978
		CNNVD-202205-3081
		CNNVD-202205-3082
		CNNVD-202205-3083
		CNNVD-202205-3084
		CNNVD-202205-3085
		CNNVD-202205-3086
		CNNVD-202205-3087
		CNNVD-202205-3088
		CNNVD-202205-3089
		CNNVD-202205-3090
		CNNVD-202205-3091
		CNNVD-202205-3092
		CNNVD-202205-3093
		CNNVD-202205-3094
		CNNVD-202205-3095
		CNNVD-202205-3096
		CNNVD-202205-3097
		CNNVD-202205-3098
		CNNVD-202205-3099

		CNNVD-202205-3100	
		CNNVD-202205-3102	
		CNNVD-202205-3152	
		CNNVD-202205-3154	
		CNNVD-202205-3156	
		CNNVD-202205-3157	
		CNNVD-202205-3158	
		CNNVD-202205-3159	
		CNNVD-202205-3160	
		CNNVD-202205-3161	
		CNNVD-202205-3162	
		CNNVD-202205-3164	
		CNNVD-202205-3295	
		CNNVD-202205-3302	
		CNNVD-202205-3307	
		CNNVD-202205-3314	
		CNNVD-202205-3316	
		CNNVD-202205-3318	
		CNNVD-202205-3319	
		CNNVD-202205-3320	
		CNNVD-202205-3321	
		CNNVD-202205-3323	
		CNNVD-202205-3355	
		CNNVD-202205-3361	
		CNNVD-202205-3364	
		CNNVD-202205-3411	
		CNNVD-202205-3418	
		CNNVD-202205-3603	
		CNNVD-202205-3618	
		CNNVD-202205-3619	
		CNNVD-202205-3620	
		CNNVD-202205-3827	
		CNNVD-202205-3842	
		CNNVD-202205-3843	
		CNNVD-202205-3853	
		CNNVD-202205-3878	
		CNNVD-202205-3925	
		CNNVD-202205-3926	
		CNNVD-202205-4007	
		CNNVD-202205-4008	
		CNNVD-202205-4018	

		CNNVD-202205-4037	
		CNNVD-202205-4255	
	中国铭飞	CNNVD-202205-3000	
		CNNVD-202205-3001	
	崇胜网络科技	CNNVD-202205-4180	
	布雷德网络科技公司	CNNVD-202205-2505	
代码问题	Apache基金会	CNNVD-202205-2457	Hewlett Packard Enterprise OneView 代码问题漏洞（CNNVD-202205-3617）
	Charm	CNNVD-202205-2611	
	Hewlett Packard Enterprise	CNNVD-202205-3617	
	Keysight Technologies	CNNVD-202205-4241	
	Laravel	CNNVD-202205-3401	
		CNNVD-202205-3403	
	LiteSpeed	CNNVD-202205-3038	
	OpenCart	CNNVD-202205-3627	
	Siemens	CNNVD-202205-2785	
	Sourcecodesterk	CNNVD-202205-2098	
	TIBCO Software	CNNVD-202205-2829	
	WSO2	CNNVD-202205-3022	
	WordPress基金会	CNNVD-202205-3455	
	formidable	CNNVD-202205-3484	
	个人开发者	CNNVD-202205-1801	
		CNNVD-202205-1913	
		CNNVD-202205-1914	
		CNNVD-202205-2095	
		CNNVD-202205-2608	
		CNNVD-202205-2796	
		CNNVD-202205-2979	
		CNNVD-202205-3182	
		CNNVD-202205-3293	
		CNNVD-202205-3357	
		CNNVD-202205-3486	
		CNNVD-202205-3488	
		CNNVD-202205-3490	
		CNNVD-202205-3815	
		CNNVD-202205-3841	
	北京润尼尔网络科技	CNNVD-202205-2482	
	温州互引信息技术	CNNVD-202205-2485	
	顶想信息科技	CNNVD-202205-2607	
授权问题	Aruba	CNNVD-202205-3535	多款VMware产品 授权问题漏洞（CNNVD-202205-3716）
		CNNVD-202205-3537	
		CNNVD-202205-3539	

	Hewlett Packard Enterprise	CNNVD-202205-3624	
	QNAP Systems	CNNVD-202205-2487	
		CNNVD-202205-2488	
		CNNVD-202205-2489	
	Siemens	CNNVD-202205-3117	
	Sysaid Technologies	CNNVD-202205-3194	
	TECSON/GOK	CNNVD-202205-2599	
	VMware	CNNVD-202205-3716	
	个人开发者	CNNVD-202205-1919	
		CNNVD-202205-3848	
操作系统命令注入	Artica	CNNVD-202205-2462	OpenSSL 操作系统命令注入漏洞（CNNVD-202205-1962）
	Aruba	CNNVD-202205-3530	
		CNNVD-202205-3531	
		CNNVD-202205-3532	
		CNNVD-202205-3534	
		CNNVD-202205-3536	
	Belkin	CNNVD-202205-3696	
	Cambium Networks	CNNVD-202205-3056	
		CNNVD-202205-3058	
		CNNVD-202205-3061	
		CNNVD-202205-3062	
	Openssl团队	CNNVD-202205-1962	
	Tenda	CNNVD-202205-2477	
	个人开发者	CNNVD-202205-3947	
	合勤科技	CNNVD-202205-3104	
缓冲区错误	Avaya	CNNVD-202205-1943	Avaya switches 缓冲区错误漏洞（CNNVD-202205-1943）
	D-Link	CNNVD-202205-2799	
		CNNVD-202205-2801	
		CNNVD-202205-2802	
		CNNVD-202205-2803	
		CNNVD-202205-2805	
		CNNVD-202205-2806	
		CNNVD-202205-2807	
		CNNVD-202205-2808	
		CNNVD-202205-2809	
	HUAWEI	CNNVD-202205-2554	
	TOTOLINK	CNNVD-202205-2886	
		CNNVD-202205-2887	
		CNNVD-202205-2888	
		CNNVD-202205-2890	
		CNNVD-202205-2891	

		CNNVD-202205-2892	
		CNNVD-202205-2893	
		CNNVD-202205-2894	
		CNNVD-202205-2895	
	Tenda	CNNVD-202205-1958	
		CNNVD-202205-1959	
		CNNVD-202205-2107	
	Tuxera	CNNVD-202205-1872	
	个人开发者	CNNVD-202205-2150	
		CNNVD-202205-3025	
		CNNVD-202205-3348	
		CNNVD-202205-3350	
访问控制错误	F5	CNNVD-202205-2141	F5 BIG-IP 访问控制错误漏洞（CNNVD-202205-2141）
	Open Automation Software	CNNVD-202205-4133	
		CNNVD-202205-4137	
	SchedMD	CNNVD-202205-2479	
	Siemens	CNNVD-202205-3119	
		CNNVD-202205-3125	
		CNNVD-202205-3126	
	SonicWall	CNNVD-202205-3343	
	TRUMPF	CNNVD-202205-1869	
资源管理错误	Arm	CNNVD-202205-3794	Arm Mali GPU Kernel Driver 资源管理错误漏洞（CNNVD-202205-3794）
		CNNVD-202205-3796	
		CNNVD-202205-3798	
	HUAWEI	CNNVD-202205-2551	
		CNNVD-202205-2552	
	WebKitGTK	CNNVD-202205-2565	
	个人开发者	CNNVD-202205-3678	
输入验证错误	Microsoft	CNNVD-202205-2758	Microsoft Windows Network File System 输入验证错误漏洞（CNNVD-202205-2781）
		CNNVD-202205-2781	
		CNNVD-202205-2869	
	PHOENIX CONTACT	CNNVD-202205-2934	
	RESI	CNNVD-202205-3101	
	VanDyke	CNNVD-202205-1878	
	个人开发者	CNNVD-202205-2584	
		CNNVD-202205-3409	
		CNNVD-202205-3512	

1. OpenLDAP SQL 注入漏洞（CNNVD-202205-2146）

OpenLDAP 是美国 Openldap 基金会的一个轻型目录访问协议(LDAP)的开源实现。

OpenLDAP 2.x 版本至 2.5.12 之前版本、2.6.x 版本至 2.6.2 之前版本存在安全漏洞，该漏洞源于通过 LDAP 查询中的 SQL 语句在 back-sql 后端中存在 SQL 注入漏洞。

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://bugs.openldap.org/show_bug.cgi?id=9815

2. Hewlett Packard Enterprise OneView 代码问题漏洞（CNNVD-202205-3617）

Hewlett Packard Enterprise OneView 是美国惠普企业（Hewlett Packard Enterprise）公司的一款便于 IT 部门自动化管理设备的软件。

Hewlett Packard Enterprise OneView 7.0 之前版本存在安全漏洞，该漏洞源于远程服务器端存在请求伪造漏洞。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04278en_us

3. 多款 VMware 产品授权问题漏洞（CNNVD-202205-3716）

VMware Cloud Foundation 等都是美国威睿（VMware）公司的产品。VMware Cloud Foundation 是一套一体化混合云平台。VMware vRealize Automation 是一个提供自助式云服务、监管式多云自动化的管理工具。VMware Workspace One Access 是一个集中式管理控制

台，通过该控制台，可以管理用户和组、设置和管理身份验证和访问策略，以及将资源添加到目录并管理这些资源的授权。

VMware 多款产品存在授权问题漏洞，该漏洞源于处理身份验证请求时 UI 中的错误。远程攻击者利用该漏洞可以绕过身份验证过程并获得对应用程序的管理访问权限。以下产品和版本受到影响：VMware Workspace ONE Access 21.08.0.0 到 21.08.0.1 版本、VMware Identity Manager 3.3.3 到 3.3.6 版本、vRealize Automation 7.6 版本、Cloud Foundation 4.0 到 4.3.1.1 版本、vRealize Suite Lifecycle Manager 8.0 到 8.4.1 Patch 2 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.vmware.com/security/advisories/VMSA-2022-0014.html

4. OpenSSL 操作系统命令注入漏洞（CNNVD-202205-1962）

OpenSSL 是 Openssl 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。

OpenSSL 存在操作系统命令注入漏洞，该漏洞源于 c_rehash 脚本未正确清理 shell 元字符导致命令注入。攻击者利用该漏洞执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=1ad73b4d27bd8c1b369a3cd453681d3a4f1bb9b2

5. Avaya switches 缓冲区错误漏洞（CNNVD-202205-1943）

Avaya switches 是法国 Avaya 公司的一款交换机。

Avaya switches 存在安全漏洞，该漏洞源于 RADIUS 客户端实现中的边界错误。远程用户可以将特制数据传递给应用程序，触发基于堆的缓冲区溢出利用该漏洞在目标系统上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://www.armis.com/blog/tlstorm-2-nanossl-tls-library-misuse-leads-to-vulnerabilities-in-common-switches/

6. F5 BIG-IP 访问控制错误漏洞（CNNVD-202205-2141）

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。

F5 BIG-IP 存在访问控制错误漏洞，攻击者可以通过未公开的请求利用该漏洞绕过 BIG-IP 中的 iControl REST 身份验证来控制受影响的系统。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.f5.com/csp/article/K23605346

7.Arm Mali GPU Kernel Driver 资源管理错误漏洞（CNNVD-202205-3794）

Arm Mali GPU Kernel Driver 是英国 Arm 公司的一个图形处理器单元的驱动程序。

Arm Mali GPU Kernel Driver 存在安全漏洞，该漏洞源于释放后重用漏洞，以下产品及版本受到影响：Midgard r28p0 版本至 r29p0

版本，r30p0 之前版本，Bifrost r17p0 版本至 r23p0 版本，r24p0 之前版本，Valhall r19p0 版本至 r23p0 版本，r24p0 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://developer.arm.com/support/arm-security-updates

8. Microsoft Windows Network File System 输入验证错误漏洞（CNNVD-202205-2781）

Microsoft Windows Network File System 是美国微软（Microsoft）公司的一种文件共享解决方案，可让您使用 NFS 协议在运行 Windows Server 和 UNIX 操作系统的计算机之间传输文件。

Microsoft Windows Network File System 存在输入验证错误漏洞。以下产品和版本受到影响：Windows Server 2019,Windows Server 2019 (Server Core installation),Windows Server 2022,Windows Server 2022 (Server Core installation),Windows Server, version 20H2 (Server Core Installation),Windows Server 2016,Windows Server 2016 (Server Core installation),Windows Server 2008 for 32-bit Systems Service Pack 2,Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation),Windows Server 2008 for x64-based Systems Service Pack 2,Windows Server 2012 R2 (Server Core installation),Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation),Windows Server 2008 R2 for x64-based Systems Service Pack 1,Windows Server 2008 R2

for x64-based Systems Service Pack 1 (Server Core installation),Windows Server 2012,Windows Server 2012 (Server Core installation),Windows Server 2012 R2。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937

1.4.2 高危漏洞实例

2022 年 5 月高危漏洞共 734 个，其中重要漏洞实例如表 6 所示。

表 6　2022 年 5 月高危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例
SQL注入	Cambium Networks	CNNVD-202205-3060	Fortinet FortiNAC SQL注入漏洞（CNNVD-202205-2037）
	Code Projects组织	CNNVD-202205-2499	
	Code Projects组织	CNNVD-202205-3309	
	Fidelis	CNNVD-202205-3647	
	Fortinet	CNNVD-202205-2037	
	Nesote Technologies	CNNVD-202205-3982	
		CNNVD-202205-3985	
		CNNVD-202205-3988	
	Photosynthetic Technology	CNNVD-202205-2976	
	Piwigo	CNNVD-202205-2574	
		CNNVD-202205-2575	
		CNNVD-202205-4154	
	Safedog	CNNVD-202205-2838	
	ShopWind	CNNVD-202205-2987	
	WordPress基金会	CNNVD-202205-2879	
		CNNVD-202205-2881	
		CNNVD-202205-3464	
	个人开发者	CNNVD-202205-1955	
		CNNVD-202205-2099	
		CNNVD-202205-2105	
		CNNVD-202205-2472	
		CNNVD-202205-2496	

		CNNVD-202205-2576	
		CNNVD-202205-3151	
		CNNVD-202205-3289	
		CNNVD-202205-3291	
		CNNVD-202205-3292	
		CNNVD-202205-3296	
		CNNVD-202205-3297	
		CNNVD-202205-3300	
		CNNVD-202205-3301	
		CNNVD-202205-3303	
		CNNVD-202205-3305	
		CNNVD-202205-3306	
		CNNVD-202205-3308	
		CNNVD-202205-3310	
		CNNVD-202205-3311	
		CNNVD-202205-3312	
		CNNVD-202205-3313	
		CNNVD-202205-3315	
		CNNVD-202205-3317	
		CNNVD-202205-3333	
		CNNVD-202205-3334	
		CNNVD-202205-3335	
		CNNVD-202205-3359	
		CNNVD-202205-3417	
		CNNVD-202205-3824	
		CNNVD-202205-3829	
		CNNVD-202205-3995	
		CNNVD-202205-4015	
		CNNVD-202205-4034	
		CNNVD-202205-4039	
	崇胜网络科技	CNNVD-202205-4157	
		CNNVD-202205-4158	
		CNNVD-202205-4159	
		CNNVD-202205-4160	
		CNNVD-202205-4161	
		CNNVD-202205-4162	
		CNNVD-202205-4164	
		CNNVD-202205-4165	
		CNNVD-202205-4166	
		CNNVD-202205-4167	
		CNNVD-202205-4168	

		CNNVD-202205-4169	
		CNNVD-202205-4170	
		CNNVD-202205-4171	
		CNNVD-202205-4172	
		CNNVD-202205-4173	
		CNNVD-202205-4174	
		CNNVD-202205-4175	
		CNNVD-202205-4176	
		CNNVD-202205-4178	
	迅易科技	CNNVD-202205-4151	
代码问题	Acronis	CNNVD-202205-3521	Apache Tomcat 代码问题漏洞（CNNVD-202205-3290）
	Apache基金会	CNNVD-202205-2969	
		CNNVD-202205-3290	
	Aruba	CNNVD-202205-3611	
	BattlEye	CNNVD-202205-3902	
	Chris Brame	CNNVD-202205-3927	
	Cisco	CNNVD-202205-2130	
	F5	CNNVD-202205-2043	
		CNNVD-202205-2066	
		CNNVD-202205-2070	
		CNNVD-202205-2072	
		CNNVD-202205-2073	
	HCL Technologies	CNNVD-202205-3204	
		CNNVD-202205-3206	
	HUAWEI	CNNVD-202205-2553	
	InHand Networks	CNNVD-202205-3120	
	Intel	CNNVD-202205-3044	
	JGraph	CNNVD-202205-3426	
		CNNVD-202205-3541	
		CNNVD-202205-3546	
		CNNVD-202205-3701	
		CNNVD-202205-3855	
	Jenkins	CNNVD-202205-3550	
	Jfrog	CNNVD-202205-3474	
	MicroStrategy	CNNVD-202205-3299	
	MiniTool	CNNVD-202205-3846	
	Nginx	CNNVD-202205-3173	
	Open Build Service组织	CNNVD-202205-1946	
	Progress Software	CNNVD-202205-3005	
	Samsung	CNNVD-202205-1987	

	Shopizer团队	CNNVD-202205-1945	
	Siemens	CNNVD-202205-2998	
	Splunk	CNNVD-202205-2534	
	Stormshield	CNNVD-202205-3079	
	TRENDnet	CNNVD-202205-3024	
	Trend Micro	CNNVD-202205-2946	
	Vim	CNNVD-202205-2617	
	WordPress基金会	CNNVD-202205-1884	
		CNNVD-202205-1889	
		CNNVD-202205-2927	
		CNNVD-202205-3449	
		CNNVD-202205-3475	
	个人开发者	CNNVD-202205-1791	
		CNNVD-202205-1798	
		CNNVD-202205-1858	
		CNNVD-202205-1968	
		CNNVD-202205-2459	
		CNNVD-202205-2463	
		CNNVD-202205-2925	
		CNNVD-202205-2930	
		CNNVD-202205-2932	
		CNNVD-202205-3360	
		CNNVD-202205-3482	
		CNNVD-202205-3592	
		CNNVD-202205-3593	
		CNNVD-202205-3808	
		CNNVD-202205-3975	
		CNNVD-202205-4004	
	信捷	CNNVD-202205-2937	
授权问题	Apple	CNNVD-202205-4149	Apple macOS 授权问题漏洞（CNNVD-202205-4149）
	Intel	CNNVD-202205-2918	
		CNNVD-202205-2919	
	Johnson Controls	CNNVD-202205-2538	
	Ping Identity	CNNVD-202205-2126	
	Pixel&tonic	CNNVD-202205-2602	
	SchedMD	CNNVD-202205-2476	
	Splunk	CNNVD-202205-2536	
		CNNVD-202205-2537	
	VMware	CNNVD-202205-3584	
	个人开发者	CNNVD-202205-3068	
		CNNVD-202205-3615	

	友讯	CNNVD-202205-3677	
操作系统命令注入	Anaconda	CNNVD-202205-3294	SonicWall SSL-VPN SMA100 系列操作系统命令注入漏洞（CNNVD-202205-3662）
	Aruba	CNNVD-202205-3529	
	FUJITSU	CNNVD-202205-2692	
	InHand Networks	CNNVD-202205-3053	
		CNNVD-202205-3054	
		CNNVD-202205-3055	
		CNNVD-202205-3109	
		CNNVD-202205-3110	
		CNNVD-202205-3112	
	Microsoft	CNNVD-202205-4277	
	Mitrastar	CNNVD-202205-1952	
	SonicWall	CNNVD-202205-3662	
	个人开发者	CNNVD-202205-2113	
		CNNVD-202205-3860	
	联想	CNNVD-202205-3703	
缓冲区错误	Accusoft	CNNVD-202205-1920	NVIDIA GPU Display Driver 缓冲区错误漏洞（CNNVD-202205-3636）
	Adobe	CNNVD-202205-2897	
		CNNVD-202205-2898	
		CNNVD-202205-2899	
		CNNVD-202205-2900	
		CNNVD-202205-2903	
		CNNVD-202205-2904	
		CNNVD-202205-2905	
		CNNVD-202205-2906	
		CNNVD-202205-2907	
		CNNVD-202205-2908	
		CNNVD-202205-2910	
		CNNVD-202205-2912	
		CNNVD-202205-2913	
	Apple	CNNVD-202205-3383	
		CNNVD-202205-3393	
		CNNVD-202205-3395	
		CNNVD-202205-3398	
		CNNVD-202205-3408	
		CNNVD-202205-3413	
		CNNVD-202205-3416	
		CNNVD-202205-3439	
		CNNVD-202205-3452	
		CNNVD-202205-3463	
		CNNVD-202205-3479	

	CNNVD-202205-3481
	CNNVD-202205-3483
	CNNVD-202205-3485
	CNNVD-202205-3487
	CNNVD-202205-3489
	CNNVD-202205-3495
	CNNVD-202205-3496
	CNNVD-202205-3503
	CNNVD-202205-3513
	CNNVD-202205-3514
	CNNVD-202205-3516
Avaya	CNNVD-202205-1942
Cisco	CNNVD-202205-2137
Delta Electronics	CNNVD-202205-3178
FOO实验室	CNNVD-202205-2718
FUJITSU	CNNVD-202205-2096
Fuji Electric	CNNVD-202205-4207
	CNNVD-202205-4209
	CNNVD-202205-4217
GNU	CNNVD-202205-3962
	CNNVD-202205-3963
GPAC	CNNVD-202205-3660
Horner Automation	CNNVD-202205-4236
	CNNVD-202205-4237
	CNNVD-202205-4238
	CNNVD-202205-4239
Imagemagick Studio	CNNVD-202205-2614
InHand Networks	CNNVD-202205-3113
Inkscape	CNNVD-202205-3075
Intel	CNNVD-202205-3013
	CNNVD-202205-3015
	CNNVD-202205-3018
Jenkins	CNNVD-202205-3571
MediaTek	CNNVD-202205-2015
Microsoft	CNNVD-202205-3208
Moddable	CNNVD-202205-3174
Mozilla基金会	CNNVD-202205-1928
	CNNVD-202205-1929
	CNNVD-202205-4285
	CNNVD-202205-4286
	CNNVD-202205-4291

		CNNVD-202205-4298	
		CNNVD-202205-4301	
	NVIDIA	CNNVD-202205-3635	
		CNNVD-202205-3636	
		CNNVD-202205-3637	
	NetBSD基金会	CNNVD-202205-2866	
	SAP	CNNVD-202205-2731	
	Secomea	CNNVD-202205-2116	
	Siemens	CNNVD-202205-2996	
		CNNVD-202205-3131	
		CNNVD-202205-3153	
	TP-Link,Mercury,Fast	CNNVD-202205-2797	
		CNNVD-202205-2798	
	Tenda	CNNVD-202205-2569	
		CNNVD-202205-2570	
		CNNVD-202205-2571	
		CNNVD-202205-2572	
		CNNVD-202205-2573	
		CNNVD-202205-3002	
	Vim	CNNVD-202205-2618	
		CNNVD-202205-2825	
		CNNVD-202205-2826	
		CNNVD-202205-3583	
		CNNVD-202205-3585	
		CNNVD-202205-3797	
	WebKitGTK	CNNVD-202205-2567	
	个人开发者	CNNVD-202205-2081	
		CNNVD-202205-2616	
		CNNVD-202205-3329	
		CNNVD-202205-3497	
		CNNVD-202205-3877	
		CNNVD-202205-3945	
		CNNVD-202205-4208	
	吉翁电子	CNNVD-202205-3668	
		CNNVD-202205-3669	
		CNNVD-202205-3670	
		CNNVD-202205-3671	
		CNNVD-202205-3674	
		CNNVD-202205-3998	
	腾达	CNNVD-202205-3697	
访问控制错误	Fortinet	CNNVD-202205-2038	Fortinet FortiIsolator

	Fortinet	CNNVD-202205-2039	访问控制错误漏洞（CNNVD-202205-2039）
	GitLab	CNNVD-202205-2009	
	InHand Networks	CNNVD-202205-3124	
	Intel	CNNVD-202205-3003	
	Jenkins	CNNVD-202205-3570	
	Open Automation Software	CNNVD-202205-4135	
		CNNVD-202205-4136	
		CNNVD-202205-4138	
		CNNVD-202205-4141	
	SchedMD	CNNVD-202205-2478	
	个人开发者	CNNVD-202205-3978	
	合勤科技	CNNVD-202205-3996	
资源管理错误	ASUS	CNNVD-202205-2931	Google Chrome 资源管理错误漏洞（CNNVD-202205-4072）
	Adobe	CNNVD-202205-2896	
		CNNVD-202205-2909	
		CNNVD-202205-2911	
		CNNVD-202205-3008	
	Apple	CNNVD-202205-3500	
		CNNVD-202205-3517	
		CNNVD-202205-3519	
		CNNVD-202205-3520	
		CNNVD-202205-3526	
	Clamav团队	CNNVD-202205-2059	
		CNNVD-202205-2064	
		CNNVD-202205-2065	
	Ethereum	CNNVD-202205-3865	
	F5	CNNVD-202205-2056	
		CNNVD-202205-2074	
		CNNVD-202205-2097	
	Fuji Electric	CNNVD-202205-4211	
	GitLab	CNNVD-202205-2007	
	Google	CNNVD-202205-1822	
		CNNVD-202205-2852	
		CNNVD-202205-2854	
		CNNVD-202205-2855	
		CNNVD-202205-2857	
		CNNVD-202205-2858	
		CNNVD-202205-2859	
		CNNVD-202205-2860	
		CNNVD-202205-4040	
		CNNVD-202205-4042	

		CNNVD-202205-4044	
		CNNVD-202205-4052	
		CNNVD-202205-4055	
		CNNVD-202205-4058	
		CNNVD-202205-4072	
	IBM	CNNVD-202205-3588	
	Linux基金会	CNNVD-202205-3523	
		CNNVD-202205-3580	
	MediaTek	CNNVD-202205-1838	
	Microsoft	CNNVD-202205-2773	
		CNNVD-202205-2800	
	Mozilla基金会	CNNVD-202205-2525	
	Siemens	CNNVD-202205-2739	
		CNNVD-202205-3134	
	Vim	CNNVD-202205-2613	
		CNNVD-202205-3814	
	个人开发者	CNNVD-202205-1812	
		CNNVD-202205-1849	
		CNNVD-202205-3171	
	金山软件	CNNVD-202205-2721	
输入验证错误	AMD	CNNVD-202205-2841	Mitsubishi Electric MELSEC iQ-F 多款产品输入验证错误漏洞（CNNVD-202205-3688）
	Apple	CNNVD-202205-3405	
		CNNVD-202205-3412	
		CNNVD-202205-3434	
		CNNVD-202205-3460	
		CNNVD-202205-3491	
	Cisco	CNNVD-202205-2132	
	F5	CNNVD-202205-2049	
		CNNVD-202205-2077	
	Google	CNNVD-202205-2851	
	Handysoft	CNNVD-202205-3802	
	Hitachi	CNNVD-202205-1903	
	IBM	CNNVD-202205-2501	
	InHand Networks	CNNVD-202205-3105	
		CNNVD-202205-3106	
		CNNVD-202205-3107	
	Intel	CNNVD-202205-2917	
		CNNVD-202205-3017	
		CNNVD-202205-3027	
	JGraph	CNNVD-202205-3683	
	Linux基金会	CNNVD-202205-3587	

MediaTek	CNNVD-202205-1978
Microsoft	CNNVD-202205-2730
	CNNVD-202205-2737
	CNNVD-202205-2743
	CNNVD-202205-2744
	CNNVD-202205-2748
	CNNVD-202205-2749
	CNNVD-202205-2753
	CNNVD-202205-2756
	CNNVD-202205-2759
	CNNVD-202205-2770
	CNNVD-202205-2774
	CNNVD-202205-2830
	CNNVD-202205-2836
	CNNVD-202205-2847
	CNNVD-202205-2861
	CNNVD-202205-2868
	CNNVD-202205-2870
	CNNVD-202205-2872
	CNNVD-202205-2876
Mozilla基金会	CNNVD-202205-3942
Samsung	CNNVD-202205-2006
Siemens	CNNVD-202205-3137
Spring团队	CNNVD-202205-2988
三菱电机	CNNVD-202205-3688
	CNNVD-202205-3689
个人开发者	CNNVD-202205-1965
	CNNVD-202205-3362
	CNNVD-202205-3363
	CNNVD-202205-3596
	CNNVD-202205-3931
	CNNVD-202205-4025

1. Fortinet FortiNAC SQL 注入漏洞（CNNVD-202205-2037）

Fortinet FortiNAC 是美国飞塔（Fortinet）公司的一套网络访问控制解决方案。该产品主要用于网络访问控制和物联网安全防护。

Fortinet FortiNAC 8.3.7 版本到 9.2.2 版本存在 SQL 注入漏洞，该漏洞源于用户提供的数据未充分清理。远程用户可以向受影响的应用程序发送特制请求利用该漏洞在应用程序数据库中执行任意 SQL 命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://fortiguard.fortinet.com/psirt/FG-IR-22-062

2. Apache Tomcat 代码问题漏洞（CNNVD-202205-3290）

Apache Tomcat 是美国阿帕奇（Apache）基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page（JSP）的支持。

Apache Tomcat 8.5.0 到 8.5.75 版本 9.0.0.M1 到 9.0.20 版本存在安全漏洞，该漏洞源于如果 Web 应用程序在 WebSocket 连接关闭的同时发送 WebSocket 消息，则应用程序可能会在关闭后继续使用该套接字，导致数据返回错误。

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/6ckmjfb1k61dyzkto9vm2k5jvt4o7w7c

3. Apple macOS 授权问题漏洞（CNNVD-202205-4149）

Apple macOS 等都是美国苹果（Apple）公司的产品。Apple macOS 是一套专为 Mac 计算机所开发的专用操作系统。Apple macOS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。Apple macOS

Big Sur 是 macOS Big Sur 是苹果公司用于 MAC 操作系统 macOS 的第 17 个主要版本。

Apple macOS Catalina 2022-003 版本、Apple macOS Monterey 12.3 版本、Apple macOS Big Sur 11.6.5 版本存在授权问题漏洞。攻击者利用该漏洞提升权限。

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/en-us/HT213183

4. SonicWall SSL-VPN SMA100 series 操作系统命令注入漏洞（CNNVD-202205-3662）

SonicWall SSL-VPN SMA100 series 是 SonicWall 的用于安全的远程连接。一系列 VPN 连接方案。

SonicWall SSL-VPN SMA100 series 存在操作系统命令注入漏洞，该漏洞源于管理界面中的输入验证不当。经过身份验证的远程用户利用该漏洞可以将特制数据传递给应用程序，并以 root 权限在目标系统上执行任意操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0010

5. NVIDIA GPU Display Driver 缓冲区错误漏洞（CNNVD-202205-3636）

NVIDIA GPU Display Driver 是美国英伟达（NVIDIA）公司的一个用于操作系统中对显卡显示模块进行交互支持的驱动软件。

NVIDIA GPU Display Driver 存在缓冲区错误漏洞，网络上未经授权的攻击者可以通过特制着色器导致越界写入，这可能导致代码执行导致拒绝服务、特权升级、信息泄露和数据篡改。 影响的范围可能会扩展到其他组件。

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/5353

6. Fortinet FortiIsolator 访问控制错误漏洞（CNNVD-202205-2039）

Fortinet FortiIsolator 是美国 Fortinet 公司的一个为浏览器提供远程安全隔离功能的应用。该应用为 Fortinet Security Fabric 添加了额外的高级威胁防护功能，并保护关键业务数据免受网络上复杂威胁的侵害。来自 Web 的内容和文件在远程容器中访问，然后将无风险的内容呈现给用户。

FortiIsolator 2.3.2 及之前版本存在访问控制错误漏洞，该漏洞源于不正确的访问控制。经过身份验证的非特权攻击者利用此漏洞可通过重新生成 URL 重新生成 CA 证书。

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://www.fortiguard.com/psirt/FG-IR-21-040

7. Google Chrome 资源管理错误漏洞（CNNVD-202205-4072）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 存在资源管理错误漏洞，该漏洞源于 Indexed DB 组件中的释放后重用问题。远程攻击者可以诱骗受害者访问特制网页利用该漏洞可以在目标系统上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_24.html

8. Mitsubishi Electric MELSEC iQ-F 多款产品输入验证错误漏洞（CNNVD-202205-3688）

Mitsubishi Electric MELSEC iQ-F series 是日本三菱电机（Mitsubishi Electric）公司的一款可编程逻辑控制器。

Mitsubishi Electric MELSEC iQ-F 系列多个版本产品存在安全漏洞，该漏洞源于不正确的输入验证。未经身份验证的远程攻击者利用该漏洞通过发送特制数据包对产品通信造成拒绝服务问题。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-004_en.pdf

二、漏洞平台推送情况

2022 年 5 月漏洞平台推送漏洞 21729 个。

表 7　2022 年 5 月漏洞平台推送情况表

序号	漏洞平台	漏洞总量
1	漏洞盒子	10416
2	补天平台	11313
推送总计		21729

三、接报漏洞情况

2022 年 5 月接报漏洞 1826 个，其中信息技术产品漏洞（通用型漏洞）291 个，网络信息系统漏洞（事件型漏洞）1535 个。

表 8　2022 年 5 月接报漏洞情况表

序号	报送单位	漏洞数量
1	内蒙古奥创科技有限公司	362
2	道普信息技术有限公司	313
3	西安四叶草信息技术有限公司	272
4	河南听潮盛世信息技术有限公司	90
5	北京国舜科技股份有限公司	59
6	北京云测信息技术有限公司	51
7	北京云科安信科技有限公司	44
8	杭州安恒信息技术股份有限公司	40
9	山东泽鹿安全技术有限公司	31
10	北京中测安华科技有限公司	31
11	成都忆享科技有限公司	29
12	山东新潮信息技术有限公司	25
13	南京众智维信息科技有限公司	24
14	国防科技大学	22
15	北京数字观星科技有限公司	21
16	广州竞远安全技术股份有限公司	20
17	星云博创科技有限公司	20
18	广州锦行网络科技有限公司	20
19	安徽华云安科技有限公司	19
20	中瑞创信息技术（北京）有限公司	19
21	个人	17
22	内蒙古思沃科技有限公司	15
23	北京天地和兴科技有限公司	14
24	北京华云安信息技术有限公司	14
25	远江盛邦（北京）网络安全科技股份有限公司	13
26	成都典安科技有限公司	12
27	腾讯科技（北京）有限公司	12
28	中电信数智科技有限公司	12
29	江苏金盾检测技术股份有限公司	11
30	上海上讯信息技术股份有限公司	11
31	北京信联科汇科技有限公司	11
32	北京众安天下科技有限公司	10
33	中兴通讯股份有限公司	10

34	杭州孝道科技有限公司	9
35	浙江宇视科技有限公司	8
36	北京山石网科信息技术有限公司	8
37	北京天融信网络安全技术有限公司	6
38	南京禾盾信息科技有限公司	6
39	上海安识网络科技有限公司	6
40	西安交大捷普网络科技有限公司	6
41	北京启明星辰信息安全技术有限公司	6
42	北京机沃科技有限公司	6
43	新华三技术有限公司	5
44	北京时代新威信息技术有限公司	5
45	北京六方领安网络科技有限公司	5
46	三六零数字安全科技集团有限公司	5
47	北京灰度科技有限公司	5
48	江苏中新赛克工业互联网安全技术创新中心有限公司	4
49	郑州云智信安安全技术有限公司	4
50	天津市兴先道科技有限公司	4
51	普一科技有限公司	4
52	北京威努特技术有限公司	3
53	北京知道创宇信息技术股份有限公司	3
54	北京安天网络安全技术有限公司	3
55	浪潮电子信息产业股份有限公司	3
56	杭州迪普科技股份有限公司	3
57	恒安嘉新（北京）科技股份公司	2
58	北京锐服信科技有限公司	2
59	杭州默安科技有限公司	2
60	奇安星城网络安全运营服务(长沙)有限公司	2
61	长春嘉诚信息技术股份有限公司	2
62	北京京东尚科信息技术有限公司	2
63	北京永信至诚科技股份有限公司	2
64	北京城市学院	2
65	华为技术有限公司	2
66	电信研究院	1
67	成都泰瑞通信设备检测有限公司	1
68	南京国云电力有限公司	1
69	安全邦（北京）信息技术有限公司	1
70	四川劭久信息安全技术有限公司	1
71	北京安帝科技有限公司	1
72	贵州泰若数字科技有限公司	1
73	浙江木链物联网科技有限公司	1
74	西南石油大学	1

75	上海斗象信息科技有限公司	1
76	北京小佑科技有限公司	1
77	墨菲未来科技(北京)有限公司	1
78	厦门服云信息科技有限公司	1
79	奇安信网神信息技术（北京）股份有限公司	1
80	北京北大软件工程股份有限公司	1
81	中国科学院信息工程研究所	1
82	中国科学院软件研究所(智能软件研究中心)	1
报送合计		1826

四、重大漏洞通报

4.1 F5 BIG-IP 访问控制错误漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于F5 BIG-IP 访问控制错误漏洞（CNNVD-202205-2141、CVE-2022-1388）情况的报送。攻击者可在未授权的情况下远程执行命令、创建或删除文件、开启或关闭服务等。F5 BIG-IP 16.1.0-16.1.2 版本、15.1.0-15.1.5 版本、14.1.0-14.1.4 版本、13.1.0-13.1.4 版本、12.1.0 - 12.1.6 版本、11.6.1-11.6.5 版本等多个版本均受此漏洞影响。目前，F5 官方已经发布了新版本修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

. 漏洞介绍

F5 BIG-IP是美国F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。F5 BIG-IP中存在访问控制错误漏洞，该漏洞是由于iControl REST的身份验证功能存在缺

陷，攻击者可利用该漏洞绕过身份验证，对目标系统远程执行命令、创建或删除文件、开启或关闭服务等。

. 危害影响

F5 BIG-IP 16.1.0-16.1.2 版本、15.1.0-15.1.5 版本、14.1.0-14.1.4 版本、13.1.0-13.1.4 版本、12.1.0 - 12.1.6 版本、11.6.1-11.6.5 版本等多个版本均受此漏洞影响。

. 修复建议

目前，F5 官方已经发布了新版本修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

https://downloads.f5.com

4.2 微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，其中微软产品本身漏洞 75 个，影响到微软产品的其他厂商漏洞 1 个。包括Microsoft Windows LDAP 输入验证错误漏洞（CNNVD-202205-2869、CVE-2022-22012）、Microsoft Windows Network File System 输入验证错误漏洞（CNNVD-202205-2781、CVE-2022-26937）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，微软官方已经发布了漏洞修复补丁，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

2022 年 5 月 10 日，微软发布了 2022 年 5 月份安全更新，共 76 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Microsoft Windows 和 Windows 组件、Microsoft Windows ALPC、Windows Failover Cluster Automation Server、Microsoft Graphics Component、Microsoft Excel、Microsoft Windows WLAN Auto Config Service等。CNNVD对其危害等级进行了评价，其中超危漏洞 3 个，高危漏洞 50 个，中危漏洞 22 个，低危漏洞 1 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 73 个新增漏洞的补丁程序，其中超危漏洞 3 个，高危漏洞 47 个，中危漏洞 22 个，低危漏洞 1 个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	官方链接
1	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2869	CVE-2022-22012	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22012
2	Microsoft Windows Network File System 输入验证错误漏洞	CNNVD-202205-2781	CVE-2022-26937	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937
3	Microsoft Windows	CNNVD-202205-2758	CVE-2022-29130	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29130

	LDAP 输入验证错误漏洞				
4	Microsoft Windows Point-to-Point Tunneling Protocol 竞争条件问题漏洞	CNNVD-202205-2865	CVE-2022-21972	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21972
5	Microsoft Exchange Server 权限许可和访问控制问题漏洞	CNNVD-202205-2736	CVE-2022-21978	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978
6	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2876	CVE-2022-22013	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22013
7	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2868	CVE-2022-22014	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22014
8	Microsoft Windows PlayToManager 竞争条件问题漏洞	CNNVD-202205-2873	CVE-2022-22016	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22016
9	Microsoft Remote Desktop Client 输入验证错误漏洞	CNNVD-202205-2872	CVE-2022-22017	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017
10	Microsoft Windows Remote	CNNVD-202205-2870	CVE-2022-22019	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22019

	Procedure Call Runtime 输入验证错误漏洞				
11	Microsoft Visual Studio 和 Microsoft .NET 输入验证错误漏洞	CNNVD-202205-2800	CVE-2022-23267	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23267
12	Microsoft Windows Point-to-Point Tunneling Protocol 竞争条件问题漏洞	CNNVD-202205-2863	CVE-2022-23270	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23270
13	Microsoft Windows ALPC 竞争条件问题漏洞	CNNVD-202205-2856	CVE-2022-23279	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23279
15	Microsoft Windows Authentication Methods 安全特征问题漏洞	CNNVD-202205-2853	CVE-2022-26913	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26913
16	Microsoft Windows Active Directory 权限许可和访问控制问题漏洞	CNNVD-202205-2850	CVE-2022-26923	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26923
17	Microsoft Local Security	CNNVD-202205-2846	CVE-2022-26925	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26925

	Authority Server 安全漏洞				
18	Microsoft Windows Address Book 输入验证错误漏洞	CNNVD-202205-2836	CVE-2022-26926	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26926
19	Microsoft Graphics Component 输入验证错误漏洞	CNNVD-202205-2830	CVE-2022-26927	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26927
20	Microsoft Windows Kerberos 权限许可和访问控制问题漏洞	CNNVD-202205-2812	CVE-2022-26931	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26931
21	Microsoft Windows Storage Spaces Controller 权限许可和访问控制问题漏洞	CNNVD-202205-2804	CVE-2022-26932	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26932
22	Microsoft Windows Storage Spaces Controller 竞争条件问题漏洞	CNNVD-202205-2780	CVE-2022-26938	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26938
23	Microsoft Windows Storage Spaces Controlle	CNNVD-202205-2779	CVE-2022-26939	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26939

	r 竞争条件问题漏洞				
24	Microsoft Windows Remote Access Connection Manager 权限许可和访问控制问题漏洞	CNNVD-202205-2776	CVE-2022-29103	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29103
25	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-202205-2775	CVE-2022-29104	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29104
26	Microsoft Windows Media 输入验证错误漏洞	CNNVD-202205-2774	CVE-2022-29105	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29105
27	Microsoft Hyper-V 竞争条件问题漏洞	CNNVD-202205-2772	CVE-2022-29106	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29106
28	Microsoft SharePoint Server 输入验证错误漏洞	CNNVD-202205-2730	CVE-2022-29108	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108
29	Microsoft Excel 输入验证错误漏洞	CNNVD-202205-2737	CVE-2022-29109	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29109
30	Microsoft Excel 输入验证错	CNNVD-202205-2861	CVE-2022-29110	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110

	误漏洞				
31	Microsoft Windows 竞争条件问题漏洞	CNNVD-202205-2769	CVE-2022-29113	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29113
32	Microsoft Windows Fax services 输入验证错误漏洞	CNNVD-202205-2767	CVE-2022-29115	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29115
33	Microsoft Visual Studio 和 Microsoft .NET 输入验证错误漏洞	CNNVD-202205-2773	CVE-2022-29117	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29117
34	Microsoft Windows Push Notifications 竞争条件问题漏洞	CNNVD-202205-2761	CVE-2022-29125	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29125
35	Microsoft Tablet Windows User Interface 竞争条件问题漏洞	CNNVD-202205-2760	CVE-2022-29126	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29126
36	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2759	CVE-2022-29128	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29128
37	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2756	CVE-2022-29129	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29129
38	Microsoft Windows	CNNVD-202205-2753	CVE-2022-29131	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29131

	LDAP 输入验证错误漏洞				
39	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-202205-2755	CVE-2022-29132	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29132
40	Microsoft Windows Kernel 权限许可和访问控制问题漏洞	CNNVD-202205-2752	CVE-2022-29133	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29133
41	Microsoft Windows Cluster Shared Volume 竞争条件问题漏洞	CNNVD-202205-2751	CVE-2022-29135	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29135
42	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2748	CVE-2022-29137	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29137
43	Microsoft Windows Cluster Shared Volume 竞争条件问题漏洞	CNNVD-202205-2750	CVE-2022-29138	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29138
44	Microsoft Windows LDAP 输入验证错误漏洞	CNNVD-202205-2749	CVE-2022-29139	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29139
4	Microsoft	CNNVD-202	CVE-2022	高	https://msrc.microsoft.com/update-guide/vuln

5	Windows LDAP 输入验证错误漏洞	205-2743	-29141	危	erability/CVE-2022-29141
46	Microsoft Windows Kernel 竞争条件问题漏洞	CNNVD-202205-2747	CVE-2022-29142	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29142
47	Microsoft Visual Studio 和 Microsoft .NET 输入验证错误漏洞	CNNVD-202205-2770	CVE-2022-29145	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29145
48	Microsoft Visual Studio 输入验证错误漏洞	CNNVD-202205-2744	CVE-2022-29148	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29148
49	Microsoft Windows Cluster Shared Volume 竞争条件问题漏洞	CNNVD-202205-2742	CVE-2022-29150	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29150
50	Microsoft Windows Cluster Shared Volume 竞争条件问题漏洞	CNNVD-202205-2746	CVE-2022-29151	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29151
51	Microsoft Visual Studio Code 输入验证错误漏洞	CNNVD-202205-2847	CVE-2022-30129	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30129
52	Microsoft Graphics Compone	CNNVD-202205-2877	CVE-2022-22011	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22011

	nts 信息泄露漏洞				
53	Microsoft Windows Remote Desktop Protocol 信息泄露漏洞	CNNVD-202205-2874	CVE-2022-22015	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22015
54	Microsoft Hyper-V 竞争条件问题漏洞	CNNVD-202205-2867	CVE-2022-22713	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22713
55	Microsoft Hyper-V 安全特征问题漏洞	CNNVD-202205-2849	CVE-2022-24466	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24466
56	Microsoft Windows Remote Access Connection Manager 信息泄露漏洞	CNNVD-202205-2823	CVE-2022-26930	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26930
57	Microsoft Windows NTFS 信息泄露漏洞	CNNVD-202205-2794	CVE-2022-26933	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26933
58	Microsoft Graphics Component 信息泄露漏洞	CNNVD-202205-2784	CVE-2022-26934	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26934
59	Microsoft Windows WLAN Auto Config Service 信息泄露漏洞	CNNVD-202205-2783	CVE-2022-26935	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26935

60	Microsoft Windows Server Service 信息泄露漏洞	CNNVD-202205-2782	CVE-2022-26936	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26936
61	Microsoft Remote Desktop Client 信息泄露漏洞	CNNVD-202205-2778	CVE-2022-26940	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26940
62	Windows Failover Cluster Automation Server 信息泄露漏洞	CNNVD-202205-2777	CVE-2022-29102	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29102
63	Microsoft Office 安全特征问题漏洞	CNNVD-202205-2740	CVE-2022-29107	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29107
64	Microsoft Graphics Component 信息泄露漏洞	CNNVD-202205-2771	CVE-2022-29112	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29112
65	Microsoft Windows Print Spooler Components 信息泄露漏洞	CNNVD-202205-2768	CVE-2022-29114	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29114
66	Microsoft Windows Kernel 信息泄露漏洞	CNNVD-202205-2766	CVE-2022-29116	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29116
67	Microsoft Windows Cluster Shared	CNNVD-202205-2765	CVE-2022-29120	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29120

	Volume 信息泄露漏洞				
68	Microsoft Windows WLAN AutoConfig Service 输入验证错误漏洞	CNNVD-202205-2763	CVE-2022-29121	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29121
69	Microsoft Windows Cluster Shared Volume 信息泄露漏洞	CNNVD-202205-2764	CVE-2022-29122	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29122
70	Microsoft Windows Cluster Shared Volume 信息泄露漏洞	CNNVD-202205-2762	CVE-2022-29123	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29123
71	Microsoft Windows BitLocker 安全特征问题漏洞	CNNVD-202205-2757	CVE-2022-29127	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29127
72	Microsoft Windows Cluster Shared Volume 信息泄露漏洞	CNNVD-202205-2754	CVE-2022-29134	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29134
73	Microsoft Windows Print Spooler Components 信息泄露漏洞	CNNVD-202205-2745	CVE-2022-29140	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29140
7	Microsoft	CNNVD-202	CVE-2022	低	https://msrc.microsoft.com/update-guide/vuln

4	.NET Framework 输入验证错误漏洞	205-2790	-30130	危	erability/CVE-2022-30130

此次更新共包括 2 个更新漏洞的补丁程序，其中高危漏洞 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 安全漏洞	CNNVD-202204-3059	CVE-2022-24513	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24513
2	Microsoft Windows PowerShell 权限许可和访问控制问题漏洞	CNNVD-202204-3062	CVE-2022-26788	高危	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26788

此次更新共包括 1 个影响微软产品的其他厂商漏洞的补丁程序，其中高危漏洞 1 个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	厂商	官方链接
1	Google Chrome 安全漏洞	CNNVD-202203-2278	CVE-2022-1096	高危	Google	https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html

． 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