北京师范大学网络信息安全通告

2021 年 4 月报告

北京师范大学信息网络中心

2021 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，2021 年 4 月份新增安全漏洞共 1880 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 179 个；从漏洞类型来看，输入验证错误类的漏洞占比最大，达到 10.80%。本月新增漏洞中，超危漏洞 264 个、高危漏洞 752 个、中危漏洞 794 个、低危漏洞 70 个，相应修复率分别为 78.03%、90.43%、89.80%以及 95.71%。合计 1666 个漏洞已有修复补丁发布，本月整体修复率 88.62%。

截至 2021 年 04 月 30 日，CNNVD 采集漏洞总量已达 162146 个。

1.1 漏洞增长概况

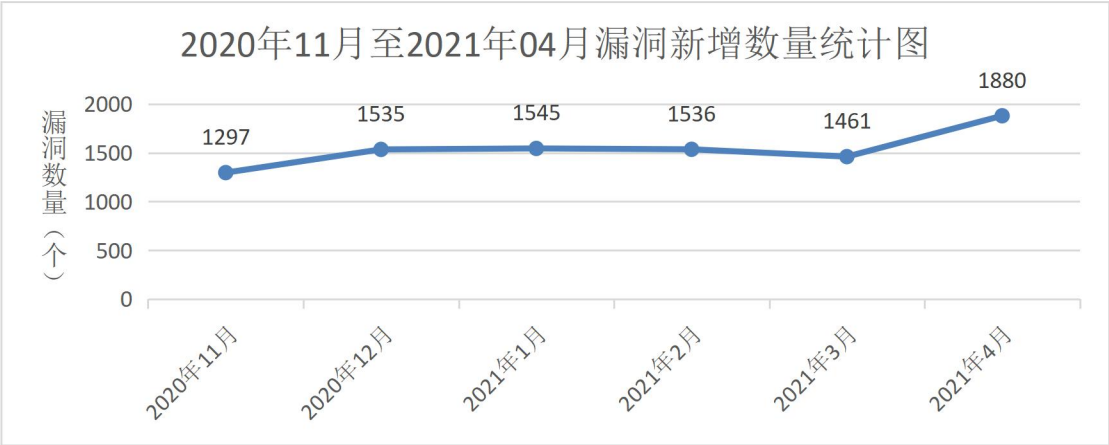

图 1 2020 年 11 月至 2021 年 4 月漏洞新增数量统计图

2021 年 4 月新增安全漏洞 1880 个，与上月（1461 个）相比增加了 28.68%。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 1542 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，Oracle 公司漏洞达到 179 个，占本月漏洞总量的 9.52%。

表 1　2021 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	Oracle	179	9.52%
2	微软	108	5.74%
3	苹果	87	4.63%
4	WordPress 基金会	78	4.15%
5	谷歌	57	3.03%
6	Juniper Networks	53	2.82%
7	Mozilla 基金会	50	2.66%
8	思科	47	2.50%
9	ASUS	38	2.02%
10	Git	28	1.49%

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 59 个，占主流操作系统漏洞总量的 11.85%，排名第一。

表 2　2021 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	59
2	Windows Server 2019	58
3	Windows Server 2016	50

4	Windows Server 2012	45
5	Windows Server 2012 R2	45
6	Windows 8.1	45
7	Windows Rt 8.1	44
8	Windows Server 2008	40
9	Windows Server 2008 R2	40
10	Windows 7	40
11	Android	22
12	Linux Kernel	10

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，其中输入验证错误类漏洞所占比例最大，约为 10.80%。

表 3 2021 年 4 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	输入验证错误	203	10.80%
2	跨站脚本	186	9.89%
3	缓冲区错误	160	8.51%
4	代码问题	112	5.96%
5	资源管理错误	73	3.88%
6	信息泄露	69	3.67%
7	SQL 注入	68	3.62%
8	代码注入	61	3.24%
9	安全特征问题	45	2.39%
10	访问控制错误	44	2.34%
11	路径遍历	44	2.34%
12	权限许可和访问控制问题	41	2.18%
13	跨站请求伪造	36	1.91%
14	授权问题	31	1.65%
15	操作系统命令注入	30	1.60%
16	命令注入	27	1.44%
17	信任管理问题	15	0.80%
18	竞争条件问题	14	0.74%
19	数据伪造问题	11	0.59%
20	注入	10	0.53%
21	日志信息泄露	6	0.32%
22	加密问题	5	0.27%
23	参数注入	5	0.27%

24	后置链接	4	0.21%
25	数字错误	3	0.16%
26	格式化字符串错误	2	0.11%
27	其他	575	30.59%

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 264 条，占本月漏洞总数的 14.04%。

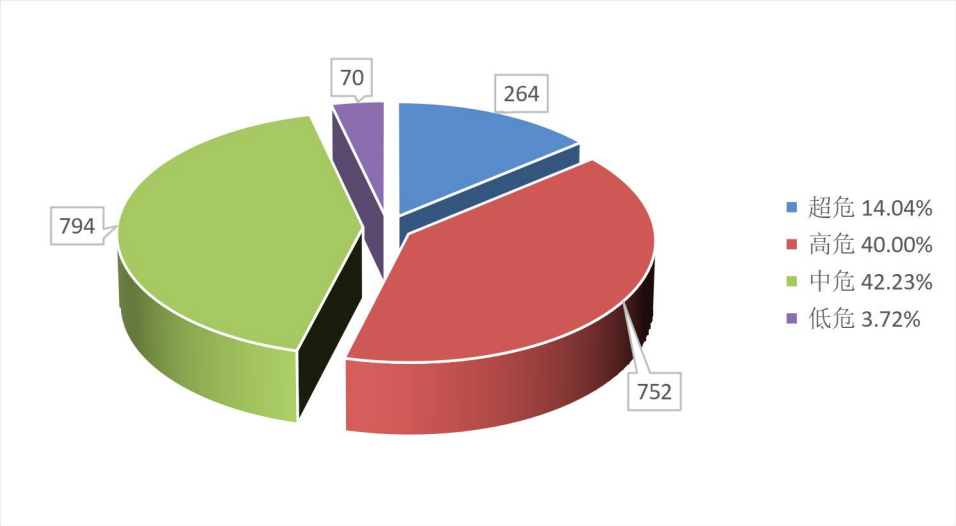

图 2　2021 年 4 月漏洞危害等级分布

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。其中低危漏洞修复率最高，达到 95.71%，超危漏洞修复率最低，比例为 78.03%。

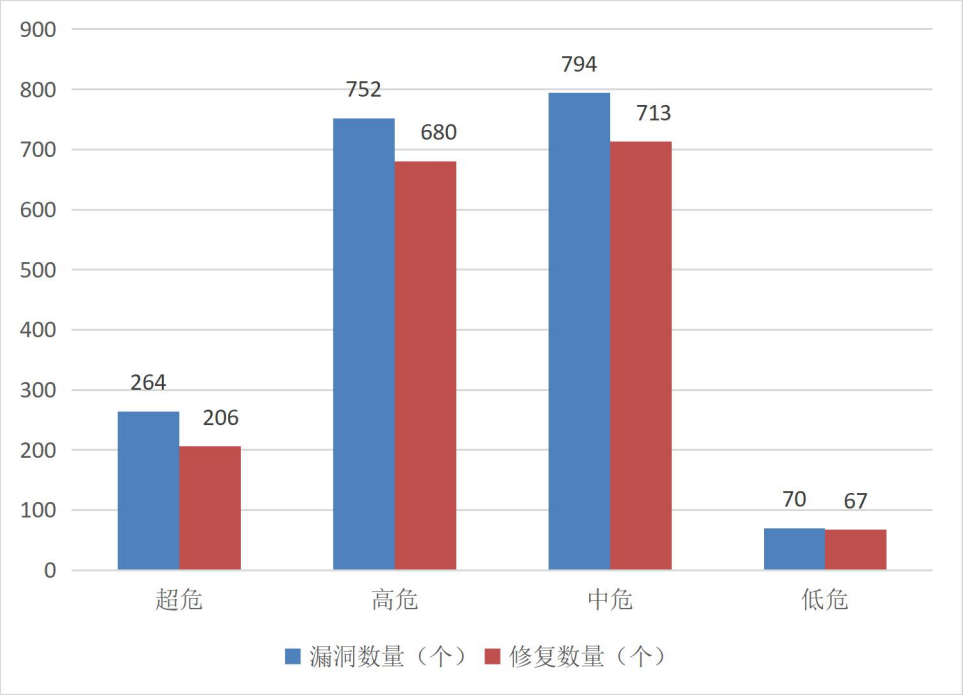

图 3　2021 年 4 月漏洞修复数量统计

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 Oracle、微软、苹果等十个厂商共 725 条漏洞，占本月漏洞总数的 38.56%，漏洞修复率为 98.48%，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 Oracle、微软、苹果、WordPress 基金会、Juniper Networks、思科、ASUS 等公司本月漏洞修复率均为 100%，共 714 条漏洞已全部修复。

表 4　2021 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	Oracle	179	179	100.00%
2	微软	108	108	100.00%
3	苹果	87	87	100.00%
4	WordPress 基金会	78	78	100.00%
5	谷歌	57	56	98.25%
6	Juniper Networks	53	53	100.00%
7	Mozilla 基金会	50	47	94.00%
8	思科	47	47	100.00%

9	ASUS	38	38	100.00%
10	Git	28	21	75.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 264 个，其中重要漏洞实例如表 5 所示。

表 5　2021 年 4 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	Django 基金会	CNNVD-202104-1148	Rockwell Automation FactoryTalk AssetCentre SQL 注入漏洞（CNNVD-202104-052）
		Inxedu	CNNVD-202104-2181	
		Nagios	CNNVD-202104-480	
		PHPSHE	CNNVD-202104-2084	
		威联通	CNNVD-202104-1223	
		Rockwell Automation	CNNVD-202104-054	
			CNNVD-202104-052	
			CNNVD-202104-055	
		SOURCEFORGE	CNNVD-202104-110	
		Vtiger	CNNVD-202104-2220	
		ZEROF	CNNVD-202104-928	
		个人开发者	CNNVD-202104-429	
			CNNVD-202104-991	
			CNNVD-202104-925	
			CNNVD-202104-992	
			CNNVD-202104-945	
			CNNVD-202104-943	
			CNNVD-202104-1088	
			CNNVD-202104-944	
			CNNVD-202104-929	
			CNNVD-202104-1213	
			CNNVD-202104-596	
			CNNVD-202104-2081	
			CNNVD-202104-994	
2	代码问题	Apache 基金会	CNNVD-202104-1187	Apache Solr 代码问题漏洞（CNNVD-202104-914）
			CNNVD-202104-2038	
			CNNVD-202104-914	
		Automattic	CNNVD-202104-153	
		Daniel Fahlke	CNNVD-202104-1583	
		Dell	CNNVD-202104-653	

		Eaton	CNNVD-202104-898	
		Matteo Piovanelli	CNNVD-202104-1122	
		Ocproducts	CNNVD-202104-304	
		PHP 社区	CNNVD-202104-2003	
		Rockwell Automation	CNNVD-202104-064	
			CNNVD-202104-051	
			CNNVD-202104-067	
			CNNVD-202104-063	
		Vangene	CNNVD-202104-341	
		WordPress 基金会	CNNVD-202104-1680	
		Wordpress 基金会	CNNVD-202104-673	
			CNNVD-202104-677	
			CNNVD-202104-136	
			CNNVD-202104-674	
		ZOHO	CNNVD-202104-1670	
		个人开发者	CNNVD-202104-127	
			CNNVD-202104-1127	
			CNNVD-202104-1535	
3	授权问题	Elementor 团队	CNNVD-202104-149	Vmware Carbon Black Cloud 授权问题漏洞（CNNVD-202104-062）
		Helpcom	CNNVD-202104-1556	
		Micro Focus	CNNVD-202104-491	
		PEGA	CNNVD-202104-2150	
		Pulse Secure	CNNVD-202104-1517	
		Sourcecodester	CNNVD-202104-632	
		Subreddit 社区	CNNVD-202104-2009	
		Vmware	CNNVD-202104-062	
4	操作系统命令注入	友讯	CNNVD-202104-073	NEC Aterm WG2600HS 操作系统命令注入漏洞（CNNVD-202104-624）
			CNNVD-202104-1093	
		NEC	CNNVD-202104-624	
		Rockwell Automation	CNNVD-202104-058	
		腾达	CNNVD-202104-1198	
			CNNVD-202104-1163	
		Totolink	CNNVD-202104-1152	
			CNNVD-202104-1066	
		个人开发者	CNNVD-202104-2221	
			CNNVD-202104-1534	
5	缓冲区错误	Ambarella	CNNVD-202104-2295	Google Android 缓冲区错误漏洞（CNNVD-202104-188）
		思科	CNNVD-202104-456	
			CNNVD-202104-451	
			CNNVD-202104-436	

			CNNVD-202104-433	
		Coreftp	CNNVD-202104-163	
		普联	CNNVD-202104-1092	
			CNNVD-202104-430	
			CNNVD-202104-078	
		Facebook	CNNVD-202104-369	
		谷歌	CNNVD-202104-188	
		Mozilla 基金会	CNNVD-202104-397	
		NLnet Labs 基金会	CNNVD-202104-2023	
			CNNVD-202104-2033	
		Open Design Alliance	CNNVD-202104-1874	
		Perforce Software	CNNVD-202104-920	
		Qualcomm	CNNVD-202104-228	
			CNNVD-202104-217	
			CNNVD-202104-216	
		RIOT	CNNVD-202104-385	
		三星	CNNVD-202104-612	
		西门子	CNNVD-202104-934	
			CNNVD-202104-984	
			CNNVD-202104-988	
		Synology	CNNVD-202104-1108	
		Valve	CNNVD-202104-631	
		Wind River	CNNVD-202104-915	
			CNNVD-202104-916	
		amazon	CNNVD-202104-1172	
		个人开发者	CNNVD-202104-382	
			CNNVD-202104-1607	
6	访问控制错误	Apache 基金会	CNNVD-202104-1824	WordPress 插件 访问控制错误漏洞（CNNVD-202104-679）
		友讯	CNNVD-202104-698	
		Lex Li	CNNVD-202104-1580	
		Solarwinds	CNNVD-202104-1068	
		Wordpress 基金会	CNNVD-202104-679	
		Zzcms 团队	CNNVD-202104-477	
		个人开发者	CNNVD-202104-1102	
			CNNVD-202104-406	
7	资源管理错误	谷歌	CNNVD-202104-1154	Google Chrome 资源管理错误漏洞（CNNVD-202104-1154）
			CNNVD-202104-1514	
		Mozilla 基金会	CNNVD-202104-037	
			CNNVD-202104-637	
			CNNVD-202104-1110	

			CNNVD-202104-463	
			CNNVD-202104-398	
			CNNVD-202104-396	
		个人开发者	CNNVD-202104-930	
8	输入验证错误	ARM	CNNVD-202104-2214	Oracle Secure Global Desktop 输入验证错误漏洞（CNNVD-202104-1523）
			CNNVD-202104-2212	
			CNNVD-202104-2209	
		Amazon	CNNVD-202104-1668	
			CNNVD-202104-1666	
		Apache 基金会	CNNVD-202104-2200	
			CNNVD-202104-2199	
		Cesanta Software	CNNVD-202104-2201	
		Eaton	CNNVD-202104-949	
			CNNVD-202104-901	
		GitLab	CNNVD-202104-1685	
		谷歌	CNNVD-202104-1520	
		MediaTek LinkIt	CNNVD-202104-2217	
		Mozilla 基金会	CNNVD-202104-641	
		NLnet Labs 基金会	CNNVD-202104-2026	
			CNNVD-202104-2025	
			CNNVD-202104-2021	
			CNNVD-202104-2028	
			CNNVD-202104-2020	
		NXP	CNNVD-202104-2198	
			CNNVD-202104-2184	
		Open Connectivity Foundation 基金会	CNNVD-202104-1528	
		Oracle	CNNVD-202104-1465	
			CNNVD-202104-1426	
			CNNVD-202104-1523	
			CNNVD-202104-1399	
			CNNVD-202104-1363	
			CNNVD-202104-1360	
		RIOT	CNNVD-202104-2208	
		三星	CNNVD-202104-2205	
		Silicon Labs	CNNVD-202104-2190	
		腾讯	CNNVD-202104-2203	
		Texas Instruments	CNNVD-202104-2182	
			CNNVD-202104-2194	

			CNNVD-202104-2223	
			CNNVD-202104-2225	
			CNNVD-202104-2183	
			CNNVD-202104-2222	
			CNNVD-202104-2230	
			CNNVD-202104-2193	
		Tobesoft	CNNVD-202104-1532	
		eCosCentric	CNNVD-202104-2196	
		个人开发者	CNNVD-202104-2187	
			CNNVD-202104-131	
			CNNVD-202104-2188	

1. Rockwell Automation FactoryTalk AssetCentre SQL 注入漏洞（CNNVD-202104-052）

Rockwell Automation FactoryTalk AssetCentre 是美国罗克韦尔（Rockwell Automation）公司的一个应用系统。提供集中式工具，用于保护，管理，版本控制，跟踪和报告整个工厂中与自动化相关的资产信息。

Rockwell Automation FactoryTalk AssetCentre 中的 ArchiveService.rem service 存在 SQL 注入漏洞，该漏洞源于缺乏适当身份验证的功能。远程攻击者可利用该漏洞执行任意 SQL 语句。

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/494865

2. Apache Solr 代码问题漏洞（CNNVD-202104-914）

Apache Solr 是美国阿帕奇（Apache）基金会的一款基于 Lucene（一款全文搜索引擎）的搜索服务器。该产品支持层面搜索、垂直搜索、高亮显示搜索结果等。

Apache Solr 8.8.2 之前版本存在安全漏洞，攻击者可利用 masterUrl 参数将索引数据复制到本地内核中，从而执行恶意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/r0ddc3a82bd7523b1453cb7a5e09eb5559517145425074a42eb326b10%40%3Cannounce.apache.org%3E

3. Vmware Carbon Black Cloud 授权问题漏洞（CNNVD-202104-062）

Vmware Carbon Black Cloud 是美国 Vmware 公司的一款为云端点提供安全检查防御功能的 Sass 平台。

VMware Carbon Black Cloud Workload appliance 1.0.0 and 1.01 存在安全漏洞，攻击者可利用该漏洞查看和更改管理设置。

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-2021-0005.html

4. NEC Aterm WG2600HS 操作系统命令注入漏洞（CNNVD-202104-624）

NEC Aterm WG2600HS 是日本电气（NEC）公司的一款无线路由器。

Aterm WG2600HS: 1.5.1 版本存在安全漏洞，该漏洞允许远程攻击者在目标系统上执行任意 shell 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://jpn.nec.com/security-info/secinfo/nv21-010.html

5. Google Android 缓冲区错误漏洞（CNNVD-202104-188）

Google Android 是美国谷歌开放手持设备联盟（Google）的一套以 Linux 为基础的开源操作系统。

Google Android 11 存在缓冲区错误漏洞，以下产品及版本受到影响：Google Android 11 中的 System 10， 11 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://source.android.com/security/bulletin/2021-04-01

6. WordPress 插件访问控制错误漏洞（CNNVD-202104-679）

WordPress 插件是 WordPress 基金会的一个应用插件。

Controlled Admin Access WordPress 插件 1.5.2 版本之前存在安全漏洞，该漏洞源于网站自定义功能和全局 CMS 设置的不受控制的访问引起的，可能导致目标资源的损坏。

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/eec0f29f-a985-4285-8eed-d1855d204a20

7. Google Chrome 资源管理错误漏洞（CNNVD-202104-1154）

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，远程攻击者可利用漏洞破坏目标系统。以下产品及版本受到影响：Google Chrome: 87.0.4280.66, 87.0.4280.141, 88.0.4324.96, 88.0.4324.146, 88.0.4324.150, 88.0.4324.182, 89.0.4389.72, 89.0.4389.90, 89.0.4389.114, 89.0.4389.128。

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/2021/04/stable-channel-update-for-desktop_14.html

8. Oracle Secure Global Desktop 输入验证错误漏洞（CNNVD-202104-1523）

Oracle Secure Global Desktop（SGD）是美国甲骨文（Oracle）公司的一款桌面虚拟化产品。用户可通过该产品访问服务器托管的应用程序和桌面。

Oracle Secure Global Desktop: 5.6 存在输入验证错误漏洞，该漏洞源于在 Oracle 安全全局桌面的服务器组件中进行了不正确的输入验证。远程攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/security-alerts/cpuapr2021.html

1.4.2 高危漏洞实例

本月高危漏洞共 752 个，其中重点漏洞实例如表 6 所示。

表 6 2021 年 4 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	Aruba	CNNVD-202104-2099	Rukovoditel SQL 注入漏洞（CNNVD-202104-499）
			CNNVD-202104-2101	
			CNNVD-202104-2098	
		CITSmart	CNNVD-202104-380	
		Daniel Fahlke	CNNVD-202104-1582	
		Devolutions	CNNVD-202104-1144	
		Eaton	CNNVD-202104-953	
		Etherpad 基金会	CNNVD-202104-2056	
		Knowage	CNNVD-202104-178	
		Rockoa	CNNVD-202104-2086	
		Rukovoditel 团	CNNVD-202104-501	

		队	CNNVD-202104-502	
			CNNVD-202104-499	
		Tibco Software	CNNVD-202104-1542	
		Void	CNNVD-202104-1815	
		Wordpress 基金会	CNNVD-202104-684	
		个人开发者	CNNVD-202104-081	
			CNNVD-202104-927	
			CNNVD-202104-924	
			CNNVD-202104-2290	
2	代码问题	Adobe	CNNVD-202104-962	IBM WebSphere Application Server 代码问题漏洞（CNNVD-202104-1555）
		Apache 基金会	CNNVD-202104-2006	
		Aruba	CNNVD-202104-2166	
		Avaya	CNNVD-202104-2050	
		Cisco	CNNVD-202104-2077	
		Clamav 团队	CNNVD-202104-439	
		Dell	CNNVD-202104-657	
		Dolby	CNNVD-202104-473	
		Forcepoint	CNNVD-202104-470	
		IBM	CNNVD-202104-1555	
		INIM ELECTRONICS	CNNVD-202104-2152	
		Jenkins	CNNVD-202104-1612	
		Juniper Networks	CNNVD-202104-1023	
			CNNVD-202104-1101	
		Lenovo	CNNVD-202104-2016	
		OutSystems	CNNVD-202104-651	
		Proofpoint	CNNVD-202104-362	
		Rapid7	CNNVD-202104-1810	
		Realtek	CNNVD-202104-500	
		SAP	CNNVD-202104-712	
		西门子	CNNVD-202104-970	
		SonicWall	CNNVD-202104-593	
		Trend Micro	CNNVD-202104-931	
		Vaadin	CNNVD-202104-1834	
		WordPress 基金会	CNNVD-202104-162	
			CNNVD-202104-172	
		Wordpress 基金会	CNNVD-202104-675	
			CNNVD-202104-680	
			CNNVD-202104-1149	
			CNNVD-202104-174	
		sunkaifei	CNNVD-202104-018	

		个人开发者	CNNVD-202104-1611	
			CNNVD-202104-457	
			CNNVD-202104-606	
			CNNVD-202104-399	
			CNNVD-202104-894	
			CNNVD-202104-460	
			CNNVD-202104-1084	
			CNNVD-202104-353	
			CNNVD-202104-1613	
			CNNVD-202104-004	
			CNNVD-202104-2041	
3	授权问题	Appspace	CNNVD-202104-1130	Avfirewalls FortiWAN 授权问题漏洞（CNNVD-202104-2039）
		Avfirewalls	CNNVD-202104-2039	
		Devolutions	CNNVD-202104-005	
		F5	CNNVD-202104-2123	
		Mitsubishi Electric	CNNVD-202104-1664	
		NetIQ	CNNVD-202104-654	
		Qnap Systems	CNNVD-202104-1861	
		Red Hat	CNNVD-202104-1157	
		三星	CNNVD-202104-587	
			CNNVD-202104-586	
			CNNVD-202104-625	
			CNNVD-202104-585	
		de Consumenten bond	CNNVD-202104-101	
4	操作系统命令注入	ASUS	CNNVD-202104-311	Netgear NETGEAR R7800 操作系统命令注入漏洞（CNNVD-202104-1073）
			CNNVD-202104-313	
		Avaya	CNNVD-202104-1850	
		友讯	CNNVD-202104-1141	
			CNNVD-202104-701	
			CNNVD-202104-689	
		Dell	CNNVD-202104-713	
		FIBARO	CNNVD-202104-1334	
		Indio Networks	CNNVD-202104-608	
		Juniper Networks	CNNVD-202104-1662	
		NEC	CNNVD-202104-628	
		Netgear	CNNVD-202104-1073	
		Subreddit 社区	CNNVD-202104-2011	
		Symantec	CNNVD-202104-1521	
		Synology	CNNVD-202104-032	

		Vivotek	CNNVD-202104-2068	
		个人开发者	CNNVD-202104-2114	
5	缓冲区错误	Adobe	CNNVD-202104-951	Microsoft Office 和 Microsoft Outlook 缓冲区错误漏洞（CNNVD-202104-839）
			CNNVD-202104-948	
		苹果	CNNVD-202104-1979	
			CNNVD-202104-1953	
			CNNVD-202104-1969	
			CNNVD-202104-1987	
			CNNVD-202104-086	
			CNNVD-202104-122	
			CNNVD-202104-1949	
			CNNVD-202104-1973	
			CNNVD-202104-1968	
			CNNVD-202104-1962	
			CNNVD-202104-1966	
			CNNVD-202104-1954	
			CNNVD-202104-091	
			CNNVD-202104-1971	
		Aprelium	CNNVD-202104-490	
		Autodesk	CNNVD-202104-1324	
			CNNVD-202104-1327	
		思科	CNNVD-202104-2102	
			CNNVD-202104-455	
			CNNVD-202104-441	
			CNNVD-202104-2072	
			CNNVD-202104-2075	
			CNNVD-202104-435	
			CNNVD-202104-434	
			CNNVD-202104-458	
		Coreftp	CNNVD-202104-165	
		Delta Electronics	CNNVD-202104-1576	
			CNNVD-202104-1574	
			CNNVD-202104-1578	
		Eipstackgroup 组织	CNNVD-202104-1193	
		FFmpeg 团队	CNNVD-202104-402	
		福昕	CNNVD-202104-1897	
			CNNVD-202104-1902	
			CNNVD-202104-1895	
			CNNVD-202104-1900	
			CNNVD-202104-1898	
		谷歌	CNNVD-202104-184	
			CNNVD-202104-1910	

			CNNVD-202104-1916
			CNNVD-202104-211
			CNNVD-202104-207
			CNNVD-202104-1515
			CNNVD-202104-202
		IBM	CNNVD-202104-1823
		ISC	CNNVD-202104-2110
		Juniper Networks	CNNVD-202104-1038
			CNNVD-202104-1107
		Linux	CNNVD-202104-1610
		Linux 基金会	CNNVD-202104-1357
			CNNVD-202104-1862
		微软	CNNVD-202104-839
			CNNVD-202104-881
		Mozilla 基金会	CNNVD-202104-1339
			CNNVD-202104-635
			CNNVD-202104-045
			CNNVD-202104-634
			CNNVD-202104-633
			CNNVD-202104-639
			CNNVD-202104-1306
			CNNVD-202104-636
			CNNVD-202104-638
			CNNVD-202104-041
			CNNVD-202104-035
			CNNVD-202104-033
			CNNVD-202104-049
		Netgear	CNNVD-202104-1887
			CNNVD-202104-1071
		西门子	CNNVD-202104-998
			CNNVD-202104-950
			CNNVD-202104-947
			CNNVD-202104-946
		普联	CNNVD-202104-696
			CNNVD-202104-1096
		个人开发者	CNNVD-202104-1878
			CNNVD-202104-1602
			CNNVD-202104-346
			CNNVD-202104-1615
			CNNVD-202104-1310
			CNNVD-202104-1634
			CNNVD-202104-1635
			CNNVD-202104-1663

			CNNVD-202104-1632	
			CNNVD-202104-1099	
			CNNVD-202104-1342	
			CNNVD-202104-2144	
			CNNVD-202104-383	
			CNNVD-202104-1321	
6	访问控制错误	Alibaba	CNNVD-202104-2000	WordPress 插件访问控制错误漏洞（CNNVD-202104-683）
		Dell	CNNVD-202104-2286	
		Eclipse 基金会	CNNVD-202104-1069	
			CNNVD-202104-1060	
		F5	CNNVD-202104-2145	
		Horner Automation	CNNVD-202104-1689	
		Juniper Networks	CNNVD-202104-1349	
		MOXA	CNNVD-202104-2046	
		Nvidia	CNNVD-202104-1591	
			CNNVD-202104-1590	
		Wordpress 基金会	CNNVD-202104-685	
			CNNVD-202104-683	
		sario528	CNNVD-202104-604	
		个人开发者	CNNVD-202104-895	
			CNNVD-202104-1070	
			CNNVD-202104-1872	
7	资源管理错误	Apache	CNNVD-202104-117	Google Chrome 资源管理错误漏洞（CNNVD-202104-989）
		苹果	CNNVD-202104-1957	
			CNNVD-202104-087	
			CNNVD-202104-1958	
			CNNVD-202104-1942	
		Autodesk	CNNVD-202104-1351	
		Eclipse 基金会	CNNVD-202104-034	
		Freebsd 基金会	CNNVD-202104-411	
		谷歌	CNNVD-202104-1113	
			CNNVD-202104-187	
			CNNVD-202104-1104	
			CNNVD-202104-1135	
			CNNVD-202104-1106	
			CNNVD-202104-989	
			CNNVD-202104-200	
			CNNVD-202104-1138	
			CNNVD-202104-1125	
			CNNVD-202104-192	

			CNNVD-202104-1915	
		IBM	CNNVD-202104-1560	
		Juniper Networks	CNNVD-202104-1089	
			CNNVD-202104-1009	
			CNNVD-202104-1146	
			CNNVD-202104-1076	
		Linux 基金会	CNNVD-202104-356	
		Matrix 基金会	CNNVD-202104-1169	
		微软	CNNVD-202104-833	
		Mozilla 基金会	CNNVD-202104-047	
			CNNVD-202104-050	
			CNNVD-202104-1323	
			CNNVD-202104-043	
			CNNVD-202104-046	
			CNNVD-202104-044	
			CNNVD-202104-048	
			CNNVD-202104-1333	
		OMICRON	CNNVD-202104-1537	
		Qualcomm	CNNVD-202104-220	
			CNNVD-202104-210	
		Vaadin	CNNVD-202104-1820	
			CNNVD-202104-1841	
		个人开发者	CNNVD-202104-2180	
			CNNVD-202104-1811	
			CNNVD-202104-1614	
			CNNVD-202104-1312	
8	输入验证错误	ABB	CNNVD-202104-350	Oracle Fusion Middleware 输入验证错误漏洞（CNNVD-202104-1446）
		苹果	CNNVD-202104-1948	
			CNNVD-202104-1945	
			CNNVD-202104-1994	
			CNNVD-202104-1970	
			CNNVD-202104-1955	
		思科	CNNVD-202104-2097	
		Clamav 团队	CNNVD-202104-437	
			CNNVD-202104-442	
		Corel	CNNVD-202104-1623	
			CNNVD-202104-1624	
			CNNVD-202104-1067	
		谷歌	CNNVD-202104-837	
		Horner Automation	CNNVD-202104-1690	
		Jakob Borg	CNNVD-202104-368	
		Juniper	CNNVD-202104-1013	

		Networks	CNNVD-202104-1054	
		MediaWiki 基金会	CNNVD-202104-1636	
		微软	CNNVD-202104-733	
			CNNVD-202104-897	
			CNNVD-202104-871	
		Oracle	CNNVD-202104-1493	
			CNNVD-202104-1506	
			CNNVD-202104-1377	
			CNNVD-202104-1462	
			CNNVD-202104-1508	
			CNNVD-202104-1434	
			CNNVD-202104-1491	
			CNNVD-202104-1402	
			CNNVD-202104-1554	
			CNNVD-202104-1475	
			CNNVD-202104-1383	
			CNNVD-202104-1446	
			CNNVD-202104-1435	
			CNNVD-202104-1371	
			CNNVD-202104-1509	
			CNNVD-202104-1412	
			CNNVD-202104-1422	
			CNNVD-202104-1527	
		Qualcomm	CNNVD-202104-212	
			CNNVD-202104-231	
			CNNVD-202104-226	
			CNNVD-202104-221	
		三星	CNNVD-202104-616	
		WordPress 基金会	CNNVD-202104-135	
		Zoom	CNNVD-202104-621	
		个人开发者	CNNVD-202104-1358	
			CNNVD-202104-2202	

1. Rukovoditel SQL 注入漏洞（CNNVD-202104-499）

Rukovoditel 是 Rukovoditel 团队的一套基于 Web 的开源项目管理软件。该软件具有项目管理、客户关系管理等功能。

Rukovoditel Project Management App 2.7.2 存在 SQL 注入漏洞，

攻击者可以发出经过身份验证的 HTTP 请求来触发此漏洞。

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://www.rukovoditel.net/

2. IBM WebSphere Application Server 代码问题漏洞（CNNVD-202104-1555）

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

IBM WebSphere Application Server 存在安全漏洞，远程攻击者可利用该漏洞获取目标服务器敏感信息或消耗内存资源。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ibm.com/support/pages/node/6445481

3. Avfirewalls FortiWAN 授权问题漏洞（CNNVD-202104-2039）

Avfirewalls FortiWAN 是美国 Avfirewalls 公司的一个网络设备。用于平衡多个 WAN 连接上的 Internet 和 Intranet 流量。

FortiWAN 存在授权问题漏洞，该漏洞源于身份验证过程中的错误。以下产品及版本受到影响：FortiWAN: before 5.1.1。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.fortiguard.com/psirt/FG-IR-21-048

4. Netgear NETGEAR R7800 操作系统命令注入漏洞（CNNVD-202104-1073）

Netgear NETGEAR R7800 是美国网件（Netgear）公司的一款无

线路由器。

NETGEAR R7800 firmware 存在安全漏洞，攻击者可利用该漏洞对受影响的固件版本执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://kb.netgear.com/000062883/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Routers-Satellites-and-Extenders

5. Microsoft Office 和 Microsoft Outlook 缓冲区错误漏洞（CNNVD-202104-839）

Microsoft Office 和 Microsoft Outlook 都是美国微软（Microsoft）公司的产品。Microsoft Office 是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 Outlook 是一套电子邮件应用程序。

Microsoft Outlook 存在内存损坏漏洞。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 365 Apps for Enterprise for 32-bit Systems,Microsoft 365 Apps for Enterprise for 64-bit Systems,Microsoft Outlook 2016 (32-bit edition),Microsoft Outlook 2016 (64-bit edition),Microsoft Outlook 2013 Service Pack 1 (32-bit editions),Microsoft Outlook 2013 Service Pack 1 (64-bit editions),Microsoft Outlook 2010 Service Pack 2 (32-bit editions),Microsoft Outlook 2010 Service Pack 2 (64-bit editions),Microsoft Outlook 2013 RT 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-2021-28452

6. WordPress 插件访问控制错误漏洞（CNNVD-202104-683）

WordPress 插件是 WordPress 基金会的一个应用插件。

WordPress 插件 WpDataTables – Tables & Table Charts premium 3.4.2 之前版本存在访问控制错误漏洞，该漏洞允许经过低特权身份验证的用户篡改参数，以通过 id_key 和 id_val 参数删除同一表中存在的另一个用户的数据。

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/d953bc62-8a6f-445b-a556-bc25cdd200e3

7. Google Chrome 资源管理错误漏洞（CNNVD-202104-989）

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 Google Chrome 浏览器中的 Blink 资源管理错误使得远程攻击者可以诱骗用户访问特制的网页，并在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/2021/04/stable-channel-update-for-desktop.html

8. Oracle Fusion Middleware 输入验证错误漏洞

（CNNVD-202104-1446）

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。

Oracle Fusion Middleware Oracle Outside In Technology Outside In Filters 8.5.5 存在输入验证错误漏洞，该漏洞允许未经身份验证的攻击者通过 HTTP 进行网络访问，进而在未授权的情况下创建、删除或修改，访问关键数据。

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/cpuapr2021.html

二、接报漏洞情况

本月接报漏洞 6252 个，其中信息技术产品漏洞（通用型漏洞）319 个，网络信息系统漏洞（事件型漏洞）5933 个。

表 7 2021 年 4 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	2441
2	上海斗象信息科技有限公司	2440
3	山东新潮信息技术有限公司	308
4	北京华云安信息技术有限公司	212
5	山东华鲁科技发展股份有限公司	89
6	北京天地和兴科技有限公司	70
7	北京数字观星科技有限公司	66
8	北京安帝科技有限公司	53

9	内蒙古思沃科技有限公司	37
10	杭州海康威视数字技术股份有限公司	35
11	北京鸿腾智能科技有限公司	32
12	安徽长泰信息安全服务有限公司	30
13	北京山石网科信息技术有限公司	29
14	浙江大华技术股份有限公司	27
15	深信服科技股份有限公司	27
16	北京顶象技术有限公司 洞见安全实验室	25
17	福建经联网络技术有限公司	24
18	北京安全共识科技有限公司	24
19	北京天融信网络安全技术有限公司	21
20	星云博创摘星实验室	20
21	山东云天安全技术有限公司	20
22	广州锦行网络科技有限公司	20
23	绿盟科技集团股份有限公司安全研究部	18
24	广州竞远安全技术股份有限公司	16
25	南京众智维信息科技有限公司	15
26	北京安华金和科技有限公司	14
27	中兴通讯	12
28	任子行网络技术股份有限公司	11
29	内蒙古洞明科技有限公司	11
30	广东易东信息安全技术有限公司	10
31	北京威努特技术有限公司	9

32	中通服咨询设计研究院有限公司	7
33	个人	7
34	重庆梦之想科技有限公司	6
35	博智安全科技股份有限公司	6
36	机沃科技	5
37	恒安嘉新（北京）科技股份公司	5
38	北京江南天安科技有限公司	5
39	北京华胜久安科技有限公司	5
40	华为未然实验室	5
41	北京启明星辰信息安全技术有限公司	4
42	北京墨云科技有限公司	4
43	西北工业大学	3
44	国防科技大学	3
45	北京滴滴信息安全科技有限公司	3
46	浙江大学 307Lab	2
47	西安四叶草信息技术有限公司	2
48	浪潮电子信息产业股份有限公司	2
49	北京云测信息科技有限公司	2
50	中兴通讯 ZXIVS-VAP 视频分析平台	1
51	中电长城网际系统应用有限公司	1
52	上海大学	1
53	软件平台上海开发部	1
54	绿盟重庆办	1

55	广东东福信息技术有限公司	1
56	北京智游网安科技有限公司	1
57	北京知道创宇信息技术股份有限公司	1
58	北京星阑科技有限公司	1
59	北京天娱在线网络科技有限公司	1
报送总计		6252

三、重大漏洞预警

3.1 Google Chrome V8 engine 输入验证错误漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Google Chrome V8 engine 输入验证错误漏洞（CNNVD-202104-837、CVE-2021-21220）情况的报送。该漏洞允许远程攻击者在目标系统上执行任意代码。Chrome 90.0.4430.70、Chrome 89.0.4389.114 及以下版本均受此漏洞影响。目前，谷歌官方已发布最新版本修复了该漏洞，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

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome V8 engine 存在输入验证错误漏洞，该漏洞允许远程攻击者在目标系统上执行任意代码。远程攻击者可以创建一个特制的 web 页面，诱使用户打开它，触发整数溢出，并在目标系统上执行任意代码。

. 危害影响

Chrome 90.0.4430.70、Chrome 89.0.4389.114 及以下版本均受此漏洞影响。

. 修复建议

目前，谷歌官方已发布最新版本修复了该漏洞，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://chromereleases.googleblog.com/2021/04/stable-channel-update-for-desktop.html

3.2 Oracle WebLogic 多个安全漏洞的预警

2021 年 4 月 21 日，Oracle 官方发布了 2021 年 4 月份的安全更新，国家信息安全漏洞库（CNNVD）对其进行了收录。其中包含了 9 个与 WebLogic 相关的重要漏洞，攻击者可利用漏洞在未授权的情况下发送攻击数据,实现远程代码执行，最终控制 WebLogic 服务器。Oracle WebLogic Server12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0.0 等多个版本均受漏洞影响。目前， Oracle 官方已经发布补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

.漏洞介绍

Oracle WebLogic Server 是美国甲骨文（Oracle）公司开发的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型

开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

Oracle 官方发布了 2021 年 4 月份的安全更新，其中包含了 9 个与 WebLogic 相关的重要漏洞，具体如下：

序号	漏洞名称	CNNVD 编号	CVE 编号
1	Oracle Fusion Middleware 安全漏洞	CNNVD-202104-1365	CVE-2021-2214
2	Oracle WebLogic Server 安全漏洞	CNNVD-202104-1391	CVE-2021-2294
3	Oracle Fusion Middleware 安全漏洞	CNNVD-202104-1420	CVE-2021-2204
4	Oracle Fusion Middleware 安全漏洞	CNNVD-202104-1449	CVE-2021-2142
5	Oracle Fusion Middleware 安全漏洞	CNNVD-202104-1463	CVE-2021-2135
6	Oracle Fusion Middleware 安全漏洞	CNNVD-202104-1474	CVE-2021-2157
7	Oracle Coherence 安全漏洞	CNNVD-202104-1493	CVE-2021-2277
8	Oracle WebLogic Server 安全漏洞	CNNVD-202104-1497	CVE-2021-2211
9	Oracle WebLogic Server 安全漏洞	CNNVD-202104-1565	CVE-2021-2136

.危害影响

攻击者可利用漏洞在未授权的情况下发送攻击数据,实现远程代码执行，最终控制 WebLogic 服务器。Oracle WebLogic 12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0.0 等多个版本均受漏洞影响。具体影响范围可访问 Oracle 官方网站进行查询，官方链接如下：

https://www.oracle.com/security-alerts/cpuapr2021.html

.修复建议

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

https://www.oracle.com/security-alerts/cpuapr2021.html