北京师范大学网络信息安全通告

2021 年 3 月报告

北京师范大学信息网络中心

2021 年 4 月

目录

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2020 年 3 月份新增安全漏洞共 1461 个，从厂商分布来看，谷歌公司产品的漏洞数量最多，共发布 96 个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到 12.53%。本月新增漏洞中，超危漏洞 194 个、高危漏洞 600 个、中危漏洞 627 个、低危漏洞 40 个，相应修复率分别为 89.69%、91.83%、86.12%以及 97.50%。合计 1304 个漏洞已有修复补丁发布，本月整体修复率 89.25%。

截至 2021 年 3 月 31 日，CNNVD 采集漏洞总量已达 160266 个。

1.1 漏洞增长概况

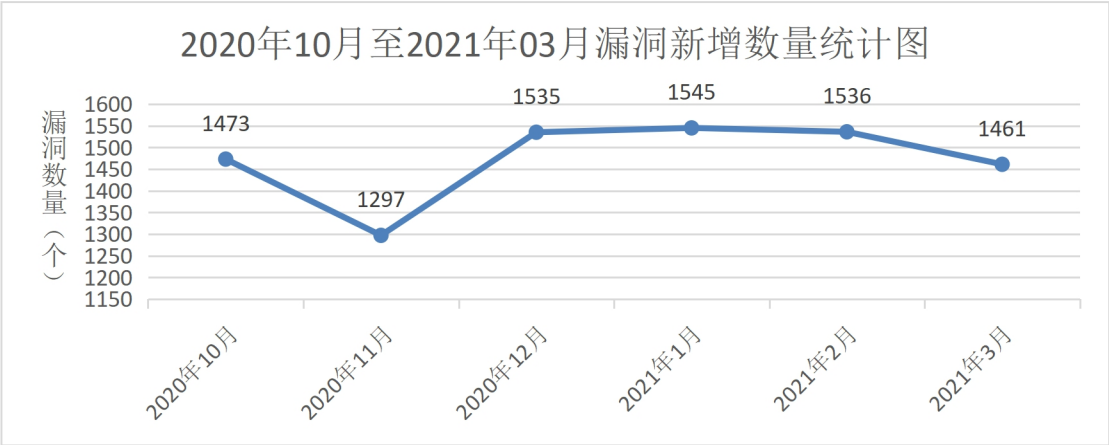

图 1 2020 年 10 月至 2021 年 3 月漏洞新增数量统计图

2020 年 3 月新增安全漏洞 1461 个，与上月（1536 个）相比减少了 4.88%。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 1475 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

3 月厂商漏洞数量分布情况如表 1 所示，谷歌公司漏洞达到 96 个，占本月漏洞总量的 6.57%。

表 1　2021 年 3 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	谷歌	96	6.57%
2	微软	91	6.23%
3	思科	59	4.04%
4	Netgear	38	2.60%
5	IBM	33	2.26%
6	三星	32	2.19%
7	Linux 基金会	31	2.12%
8	WordPress 基金会	30	2.05%
9	Red Hat	24	1.64%
10	Git	23	1.57%

1.2.2 漏洞产品分布

3 月主流操作系统的漏洞统计情况如表 2 所示。本月 Android 漏洞数量最多，共 51 个，占主流操作系统漏洞总量的 14.74%，排名第一。

表 2　2021 年 3 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Android	51
2	Windows Server 2019	42
3	Windows 10	41

4	Windows Server 2016	33
5	Windows Server 2012	27
6	Windows Server 2012 R2	27
7	Linux Kernel	24
8	Windows Server 2008	23
9	Windows Server 2008 R2	23
10	Windows 8.1	20
11	Windows Rt 8.1	19
12	Windows 7	16

1.2.3 漏洞类型分布

3 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 12.53%。

表 3 2021 年 3 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	183	12.53%
2	缓冲区错误	147	10.06%
3	代码问题	81	5.54%
4	输入验证错误	74	5.07%
5	资源管理错误	54	3.70%
6	SQL 注入	48	3.29%
7	授权问题	41	2.81%
8	信息泄露	37	2.53%
9	命令注入	36	2.46%
10	访问控制错误	31	2.12%
11	路径遍历	31	2.12%
12	跨站请求伪造	23	1.57%
13	注入	21	1.44%
14	信任管理问题	15	1.03%
15	操作系统命令注入	15	1.03%
16	代码注入	13	0.89%
17	加密问题	11	0.75%
18	权限许可和访问控制问题	8	0.55%
19	数据伪造问题	8	0.55%
20	竞争条件问题	7	0.48%
21	后置链接	6	0.41%
22	安全特征问题	5	0.34%
23	数字错误	5	0.34%

24	日志信息泄露	5	0.34%
25	参数注入	5	0.34%
26	环境问题	2	0.14%
27	默认配置问题	2	0.14%
28	配置错误	1	0.07%
29	其他	546	37.37%

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。3 月漏洞危害等级分布如图 2 所示，其中超危漏洞 194 条，占本月漏洞总数的 13.28%。

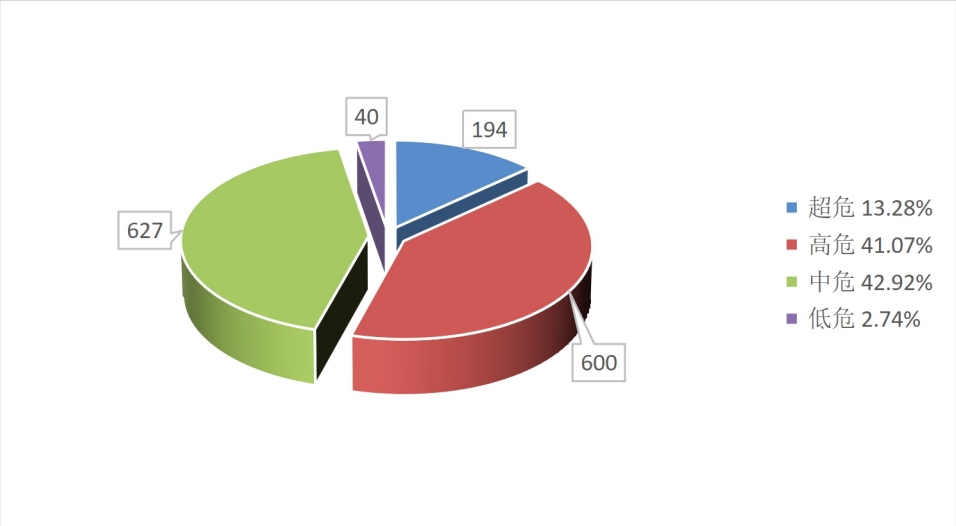

图 2　2021 年 3 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1　整体修复情况

3 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 97.50%，中危漏洞修复率最低，比例为 86.12%。

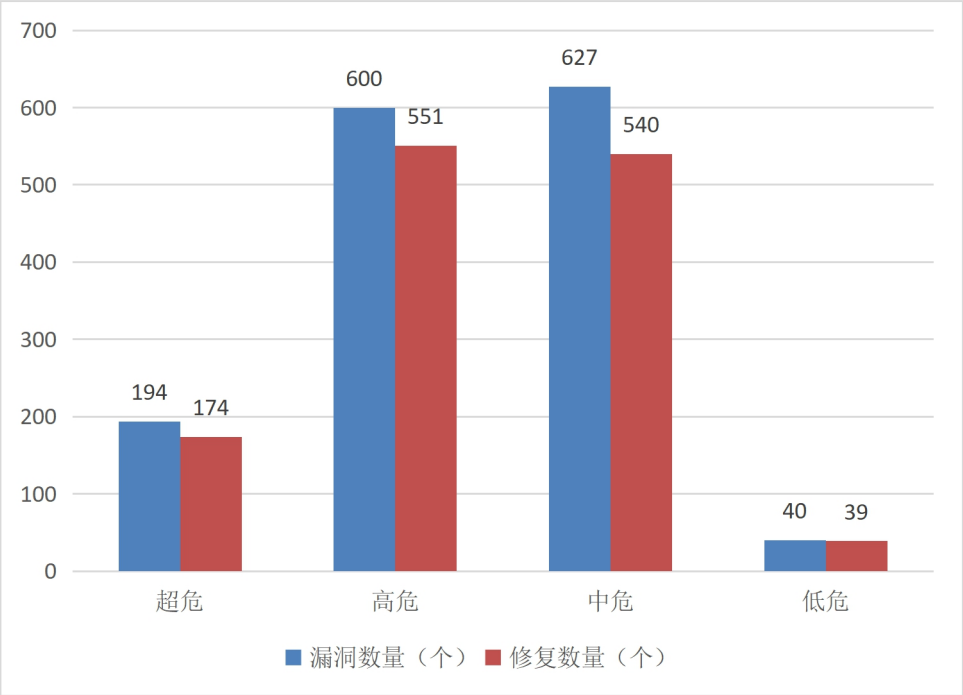

图 3　2021 年 3 月漏洞修复数量统计

1.3.2　厂商修复情况

3 月漏洞修复情况按漏洞数量前十厂商进行统计，其中谷歌、微软、思科等十个厂商共 457 条漏洞，占本月漏洞总数的 31.28%，漏洞修复率为 98.25%，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，其中谷歌、微软、思科、Netgear、IBM、三星、Linux 基金会、WordPress 基金会等公司本月漏洞修复率均为 100%，共 449 条漏洞已全部修复。

表 4　2021 年 3 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	谷歌	96	96	100.00%
2	微软	91	91	100.00%
3	思科	59	59	100.00%
4	Netgear	38	38	100.00%
5	IBM	33	33	100.00%
6	三星	32	32	100.00%
7	Linux 基金会	31	31	100.00%
8	WordPress 基金会	30	30	100.00%

9	Red Hat	24	20	83.33%
10	Git	23	19	82.61%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 194 个，其中重要漏洞实例如表 5 所示。

表 5　2021 年 3 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	Excellent Infotek Corporation	CNNVD-202103-1081	Wordpress Photo Gallery SQL 注入漏洞（CNNVD-202103-1118）
		Hgiga	CNNVD-202103-1157	
		Invigo	CNNVD-202103-1496	
		Kentico	CNNVD-202103-525	
		Matthias Van Woensel	CNNVD-202103-337	
		Sourcecodester	CNNVD-202103-1728	
		TYPO3	CNNVD-202103-990	
		Wordpress 基金会	CNNVD-202103-1118	
		Xerox	CNNVD-202103-1598	
		Zen Ventures	CNNVD-202103-1213	
		个人开发者	CNNVD-202103-1422	
			CNNVD-202103-751	
			CNNVD-202103-954	
			CNNVD-202103-294	
			CNNVD-202103-712	
			CNNVD-202103-221	
2	代码问题	Apache 基金会	CNNVD-202103-1262	VMware View Planner 代码问题漏洞（CNNVD-202103-293）
		Domainmod 社区	CNNVD-202103-972	
		Egavilan Media	CNNVD-202103-1002	
		Eprints	CNNVD-202103-029	
		LumisX	CNNVD-202103-286	
		Mulesoft	CNNVD-202103-1535	
			CNNVD-202103-1536	
		Netgear	CNNVD-202103-1562	
		Pivotal	CNNVD-202103-883	

		Software		
		Realtek	CNNVD-202103-1497	
		Sonlogger	CNNVD-202103-488	
		VMware	CNNVD-202103-293	
		WordPress 基金会	CNNVD-202103-844	
		Wordpress 基金会	CNNVD-202103-318	
		XStream 团队	CNNVD-202103-1282	
		XStream 团队	CNNVD-202103-1283	
		Xstream 团队	CNNVD-202103-1239	
			CNNVD-202103-1234	
			CNNVD-202103-1244	
			CNNVD-202103-1233	
		个人开发者	CNNVD-202103-947	
			CNNVD-202103-1459	
			CNNVD-202103-1267	
3	授权问题	DELL	CNNVD-202103-139	NETGEAR 授权问题漏洞（CNNVD-202103-1361）
		Excellent Infotek Corporation	CNNVD-202103-1090	
		Genua	CNNVD-202103-013	
		Grandstream	CNNVD-202103-1623	
		Netgear	CNNVD-202103-1362	
			CNNVD-202103-1363	
			CNNVD-202103-1361	
		Veritas Technologies	CNNVD-202103-016	
		Wordpress 基金会	CNNVD-202103-1114	
		个人开发者	CNNVD-202103-559	
			CNNVD-202103-1231	
			CNNVD-202103-564	
			CNNVD-202103-746	
4	操作系统命令注入	Apache	CNNVD-202103-1467	Apache SpamAssassin 操作系统命令注入漏洞（CNNVD-202103-1467）
		Eprints	CNNVD-202103-020	
			CNNVD-202103-014	
		LUCY	CNNVD-202103-840	
5	缓冲区错误	Aruba	CNNVD-202103-1587	Qualcomm 封闭源组件缓冲区错误漏洞 (CNNVD-202103-030)
		Cisco	CNNVD-202103-1394	
		GNU 社区	CNNVD-202103-1473	
		谷歌	CNNVD-202103-158	
			CNNVD-202103-184	

		JPEG	CNNVD-202103-126	
		Laurent Rineau	CNNVD-202103-366	
			CNNVD-202103-367	
			CNNVD-202103-365	
			CNNVD-202103-368	
		微软	CNNVD-202103-487	
		Mozilla 基金会	CNNVD-202103-480	
		Qualcomm	CNNVD-202103-032	
			CNNVD-202103-030	
			CNNVD-202103-038	
			CNNVD-202103-041	
			CNNVD-202103-045	
			CNNVD-202103-049	
			CNNVD-202103-043	
		三星	CNNVD-202103-347	
		Schneider Electric	CNNVD-202103-827	
		Tobesoft	CNNVD-202103-1443	
		Wind River	CNNVD-202103-841	
		个人开发者	CNNVD-202103-742	
			CNNVD-202103-001	
			CNNVD-202103-811	
			CNNVD-202103-744	
			CNNVD-202103-906	
		群晖科技	CNNVD-202103-920	
6	访问控制错误	Netop	CNNVD-202103-1478	Netop Vision 访问控制错误漏洞 (CNNVD-202103-1478)
		Square Box Systems	CNNVD-202103-505	
		ZyXEL	CNNVD-202103-1005	
		个人开发者	CNNVD-202103-1018	
7	资源管理错误	Facebook	CNNVD-202103-804	Google Android 资源管理错误漏洞 (CNNVD-202103-153)
		谷歌	CNNVD-202103-153	
		Mozilla 基金会	CNNVD-202103-484	
			CNNVD-202103-479	
			CNNVD-202103-481	
		个人开发者	CNNVD-202103-899	
			CNNVD-202103-898	
			CNNVD-202103-910	
		群晖科技	CNNVD-202103-902	
8	输入验证错误	Genivia	CNNVD-202103-1447	MarkAny MaEPSBroker 输入验证错误漏洞 (CNNVD-202103-1441)
		MarkAny	CNNVD-202103-1441	
		Qualcomm	CNNVD-202103-050	

		Red Hat	CNNVD-202103-524	
		个人开发者	CNNVD-202103-776	
			CNNVD-202103-123	
			CNNVD-202103-122	
			CNNVD-202103-1686	

1. Wordpress Photo Gallery SQL 注入漏洞（CNNVD-202103-1118）

Wordpress Photo Gallery 是 Wordpress 基金会开源的一个应用插件。提供一个将响应式画廊和相册添加到的网站功能。

WordPress Photo Gallery plugin 存在 SQL 注入漏洞，该漏洞源于 frontend/models/model.php bwg_search_x 参数过滤不严格导致。

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://wordpress.org/

2. VMware View Planner 代码问题漏洞（CNNVD-202103-293）

VMware View Planner 是美国 VMware 公司的一个应用软件。提供了一种可捕获部署平台的整体可扩展性以及给定桌面内每个单独的应用程序操作性能的方法。

VMware View Planner 4.x prior to 4.6 存在安全漏洞，该漏洞允许未经授权的攻击者上传和执行一个特别制作的文件，进而在 logupload 容器中远程执行代码。

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.accellion.com/products/fta/

3. NETGEAR 授权问题漏洞（CNNVD-202103-1361）

NETGEAR 是美国网件（Netgear）公司的一款路由器。连接两个或多个网络的硬件设备，在网络间起网关的作用。

Certain NETGEAR 存在安全漏洞，以下产品及版本受到影响：RBW30 before 2.6.2.2, RBS40V before 2.6.2.4, RBK852 before 3.2.17.12, RBK853 before 3.2.17.12, RBK854 before 3.2.17.12, RBR850 before 3.2.17.12, RBS850 before 3.2.17.12, RBK752 before 3.2.17.12, RBK753 before 3.2.17.12, RBK753S before 3.2.17.12, RBK754 before 3.2.17.12, RBR750 before 3.2.17.12, and RBS750 before 3.2.17.12。

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/000063017/Security-Advisory-for-Authentication-Bypass-on-Some-WiFi-Systems-PSV-2020-0492

4. Apache SpamAssassin 操作系统命令注入漏洞（CNNVD-202103-1467）

Apache SpamAssassin 是美国阿帕奇（Apache）基金会的一款开源的垃圾邮件过滤器。该产品为系统管理员提供了一个过滤器，并支持对电子邮件进行分类阻止垃圾邮件。

Apache SpamAssassin before 3.4.5 存在操作系统命令注入漏洞，该漏洞允许通过配置恶意规则配置(.cf)文件来运行系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://ubuntu.com/security/CVE-2020-1946

5. Qualcomm 封闭源组件缓冲区错误漏洞（CNNVD-202103-030）

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

Qualcomm 封闭源组件存在缓冲区错误漏洞，该漏洞可导致在播

放非标准的视频片段时，发生缓冲区溢出。

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/march-2021-bulletin

6. Netop Vision 访问控制错误漏洞（CNNVD-202103-1478）

Netop Vision 是丹麦 Netop 公司的一个应用系统。提供一个课堂管理软件。

Netop Vision Pro up to and including 9.7.1 存在访问控制错误漏洞，该漏洞允许未经身份验证的攻击者使用系统权限读写远程机器上的文件，从而导致权限升级。

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.netop.com/

7. Google Android 资源管理错误漏洞（CNNVD-202103-153）

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/Pixel 存在安全漏洞，该漏洞源于 sdp_discovery.cc 中的 sdp_copy_raw_data 的双重释放而导致系统受损，这可能导致远程代码执行。

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/pixel/2021-03-01

8. MarkAny MaEPSBroker 输入验证错误漏洞（CNNVD-202103-1441）

MarkAny MaEPSBroker 是 MarkAny 开源的一个应用程序。为当前用户添加注册表项，这将使该程序在每次重新引导时自动启动。

MaEPSBroker 2.5.0.31 存在输入验证错误漏洞，该漏洞源于解析 brokerCommand 参数时不正确的输入验证检查，导致触发命令注入漏洞。

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://www.markany.com/eng/

1.4.2 高危漏洞实例

本月高危漏洞共 600 个，其中重点漏洞实例如表 6 所示。

表 6　2021 年 3 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	Egavilan Media	CNNVD-202103-1003	WordPress plugin Paid Memberships Pro SQL 注入漏洞（CNNVD-202103-1086）
		Envato	CNNVD-202103-1112	
		HPE	CNNVD-202103-1255	
		MYBB 团队	CNNVD-202103-983	
			CNNVD-202103-981	
			CNNVD-202103-940	
			CNNVD-202103-941	
		WordPress 基金会	CNNVD-202103-1086	
		Wordpress 基金会	CNNVD-202103-1116	
			CNNVD-202103-1153	
			CNNVD-202103-1117	
			CNNVD-202103-1113	
			CNNVD-202103-1151	
			CNNVD-202103-1120	
			CNNVD-202103-1163	
			CNNVD-202103-1119	
			CNNVD-202103-1129	
			CNNVD-202103-1127	
		Zetetic	CNNVD-202103-1498	
		个人开发者	CNNVD-202103-1307	
			CNNVD-202103-1158	

			CNNVD-202103-295	
			CNNVD-202103-290	
			CNNVD-202103-1726	
			CNNVD-202103-297	
			CNNVD-202103-287	
2	代码问题	Bosch	CNNVD-202103-1494	Dell SRS Policy Manager 代码问题漏洞（CNNVD-202103-022）
			CNNVD-202103-1462	
			CNNVD-202103-1465	
			CNNVD-202103-1493	
			CNNVD-202103-1461	
			CNNVD-202103-1460	
			CNNVD-202103-1495	
		思科	CNNVD-202103-1395	
		Compass Plus	CNNVD-202103-1211	
		Dell	CNNVD-202103-888	
			CNNVD-202103-022	
		FastStone	CNNVD-202103-1132	
		GE Grid Solutions	CNNVD-202103-1011	
		IBM	CNNVD-202103-1689	
			CNNVD-202103-1662	
		Mantisbt	CNNVD-202103-539	
		NTT TechnoCross	CNNVD-202103-847	
		Privoxy 团队	CNNVD-202103-673	
		SPDK 社区	CNNVD-202103-921	
		Secomea	CNNVD-202103-516	
		Sourcecodester	CNNVD-202103-1727	
		TIBCO	CNNVD-202103-1376	
			CNNVD-202103-1314	
		Tenable Network Security	CNNVD-202103-306	
		WordPress 基金会	CNNVD-202103-1165	
		Wordpress 基金会	CNNVD-202103-1130	
		Xstream 团队	CNNVD-202103-1236	
			CNNVD-202103-1246	
			CNNVD-202103-1238	
		ZOHO	CNNVD-202103-1173	
		solarwinds	CNNVD-202103-1617	
		vmware	CNNVD-202103-1703	

		个人开发者	CNNVD-202103-1016	
			CNNVD-202103-1550	
			CNNVD-202103-1549	
			CNNVD-202103-725	
			CNNVD-202103-908	
			CNNVD-202103-959	
			CNNVD-202103-909	
3	授权问题	Atlassian	CNNVD-202103-1269	F5 BIG-IP 授权问题漏洞（CNNVD-202103-824）
		思科	CNNVD-202103-1387	
		Emerson	CNNVD-202103-701	
		F5	CNNVD-202103-824	
		GNU 社区	CNNVD-202103-233	
		Grafana 实验室	CNNVD-202103-1174	
		Micro Focus	CNNVD-202103-1492	
		Netgear	CNNVD-202103-1343	
			CNNVD-202103-733	
			CNNVD-202103-731	
		三星	CNNVD-202103-1482	
		SonicWall	CNNVD-202103-511	
		Veritas Technologies	CNNVD-202103-017	
			CNNVD-202103-015	
		个人开发者	CNNVD-202103-965	
			CNNVD-202103-803	
4	操作系统命令注入	Basercms 团队	CNNVD-202103-1543	Sonicwall SMA100 操作系统命令注入漏洞（CNNVD-202103-884）
		Dell	CNNVD-202103-553	
		Eprints	CNNVD-202103-018	
		Invigo	CNNVD-202103-1517	
		Mariadb 基金会	CNNVD-202103-1191	
		Netgear	CNNVD-202103-1560	
		Sonicwall	CNNVD-202103-884	
		个人开发者	CNNVD-202103-1657	
5	缓冲区错误	Accusoft	CNNVD-202103-1696	Google Chrome 缓冲区错误漏洞（CNNVD-202103-268）
			CNNVD-202103-1692	
			CNNVD-202103-1690	
		Adobe	CNNVD-202103-915	
			CNNVD-202103-914	
			CNNVD-202103-916	
			CNNVD-202103-894	
			CNNVD-202103-912	
			CNNVD-202103-893	
			CNNVD-202103-897	
			CNNVD-202103-896	
		Aruba	CNNVD-202103-1599	

		思科	CNNVD-202103-1399	
		Corel	CNNVD-202103-1614	
		Esri	CNNVD-202103-1500	
			CNNVD-202103-1499	
		Facebook	CNNVD-202103-801	
		FastStone	CNNVD-202103-1149	
			CNNVD-202103-1135	
			CNNVD-202103-1136	
			CNNVD-202103-1134	
		福昕	CNNVD-202103-1235	
			CNNVD-202103-1279	
			CNNVD-202103-1276	
			CNNVD-202103-1254	
		GNU 社区	CNNVD-202103-231	
			CNNVD-202103-235	
		Gigaset	CNNVD-202103-130	
		谷歌	CNNVD-202103-136	
			CNNVD-202103-274	
			CNNVD-202103-299	
			CNNVD-202103-934	
			CNNVD-202103-298	
			CNNVD-202103-134	
			CNNVD-202103-273	
			CNNVD-202103-291	
			CNNVD-202103-268	
		Linux 基金会	CNNVD-202103-1223	
			CNNVD-202103-1071	
			CNNVD-202103-521	
			CNNVD-202103-522	
		MediaArea	CNNVD-202103-1098	
		微软	CNNVD-202103-574	
		Mozilla 基金会	CNNVD-202103-1319	
			CNNVD-202103-1348	
			CNNVD-202103-490	
			CNNVD-202103-1356	
		Netgear	CNNVD-202103-1360	
			CNNVD-202103-1353	
			CNNVD-202103-1352	
			CNNVD-202103-1350	
			CNNVD-202103-735	
			CNNVD-202103-1342	
		Privoxy 团队	CNNVD-202103-671	
			CNNVD-202103-672	

		Red Hat	CNNVD-202103-344	
		Schneider Electric	CNNVD-202103-805	
			CNNVD-202103-828	
			CNNVD-202103-808	
			CNNVD-202103-806	
			CNNVD-202103-807	
		西门子	CNNVD-202103-683	
			CNNVD-202103-695	
			CNNVD-202103-697	
			CNNVD-202103-698	
		个人开发者	CNNVD-202103-486	
			CNNVD-202103-810	
			CNNVD-202103-1372	
			CNNVD-202103-819	
			CNNVD-202103-1403	
			CNNVD-202103-813	
			CNNVD-202103-809	
			CNNVD-202103-817	
			CNNVD-202103-743	
			CNNVD-202103-789	
			CNNVD-202103-816	
			CNNVD-202103-882	
			CNNVD-202103-745	
			CNNVD-202103-769	
6	访问控制错误	Eclipse 基金会	CNNVD-202103-716	Microsoft Visual Studio 后置链接漏洞（CNNVD-202103-640）
		F5	CNNVD-202103-818	
		GitHub	CNNVD-202103-246	
		Kong	CNNVD-202103-1111	
		Qualcomm	CNNVD-202103-046	
		Red Hat	CNNVD-202103-1219	
		Samsung	CNNVD-202103-372	
		Secomea	CNNVD-202103-531	
		西门子	CNNVD-202103-977	
		Wordpress 基金会	CNNVD-202103-1164	
		个人开发者	CNNVD-202103-1001	
7	资源管理错误	思科	CNNVD-202103-1386	Linux kernel 资源管理错误漏洞（CNNVD-202103-1576）
		Esri	CNNVD-202103-1475	
		福昕	CNNVD-202103-1253	
			CNNVD-202103-1249	
		GNU 社区	CNNVD-202103-230	
		谷歌	CNNVD-202103-154	
			CNNVD-202103-935	

			CNNVD-202103-159	
			CNNVD-202103-263	
			CNNVD-202103-933	
			CNNVD-202103-256	
			CNNVD-202103-161	
			CNNVD-202103-284	
			CNNVD-202103-272	
			CNNVD-202103-258	
		HedHat	CNNVD-202103-343	
		Kopano	CNNVD-202103-1708	
		Linux 基金会	CNNVD-202103-1576	
		Openbsd	CNNVD-202103-527	
		Qualcomm	CNNVD-202103-028	
			CNNVD-202103-025	
		个人开发者	CNNVD-202103-1073	
			CNNVD-202103-238	
			CNNVD-202103-239	
			CNNVD-202103-740	
			CNNVD-202103-240	
8	输入验证错误	Adobe	CNNVD-202103-792	Adobe Creative Cloud Desktop Application 输入验证错误漏洞（CNNVD-202103-792）
			CNNVD-202103-767	
		CZ.NIC	CNNVD-202103-1636	
		思科	CNNVD-202103-1450	
			CNNVD-202103-1406	
		Corel	CNNVD-202103-1595	
		Dell	CNNVD-202103-557	
		ExpressVPN	CNNVD-202103-721	
		谷歌	CNNVD-202103-162	
		Linux 基金会	CNNVD-202103-676	
		Npm	CNNVD-202103-1150	
			CNNVD-202103-1197	
		Open Source Matters 团队	CNNVD-202103-201	
		Packet Tide	CNNVD-202103-925	
		Privoxy 团队	CNNVD-202103-674	
		Quadbase	CNNVD-202103-945	
		Qualcomm	CNNVD-202103-031	
		Seth Vargo	CNNVD-202103-1732	
		TYPO3	CNNVD-202103-995	
		Weseek	CNNVD-202103-700	
		个人开发者	CNNVD-202103-548	
			CNNVD-202103-1218	
			CNNVD-202103-533	

1. WordPress plugin Paid Memberships Pro SQL 注入漏洞（CNNVD-202103-1086）

WordPress plugin Paid Memberships Pro 是 （WordPress）开源的一个应用程序插件。该插件专为优质内容网站，俱乐部/协会，订阅产品，新闻通讯等而设计。

Paid Memberships Pro versions prior to 2.5.6 存在 SQL 注入漏洞，该漏洞允许通过身份验证的远程攻击者通过未指定的矢量执行任意 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：

https://www.paidmembershipspro.com/pmpro-update-2-5-6/

2. Dell SRS Policy Manager 代码问题漏洞（CNNVD-202103-022）

Dell SRS Policy Manager 是美国戴尔（Dell）公司的一个应用软件。提供戴尔策略管理功能

SRS Policy Manager 6.X 存在安全漏洞，该漏洞源于错误配置的 XML 解析器在处理用户提供的 DTD 输入时没有进行足够的验证。攻击者可利用该漏洞做为非根用户读取系统文件，并可能暂时中断 ESRS 服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.dell.com/support/kbdoc/en-us/000183576/dsa-2021-045-dell-emc-srs-policy-manager-security-update-for-external-entity-injection-vulnerability

3. F5 BIG-IP 授权问题漏洞（CNNVD-202103-824）

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 存在授权问题漏洞，该漏洞源于群集传输服务的身份验证，以及由群集使用的所有数据用于传输的 ElasticSearch 未加密导致。

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/K34074377

4. Sonicwall SMA100 操作系统命令注入漏洞（CNNVD-202103-884）

Sonicwall SMA100 是美国 Sonicwall 公司的一款安全访问网关设备。

SonicWall SMA100 10.2.0.5 及更早版本存在操作系统命令注入漏洞，该漏洞允许经过身份验证的攻击者以“nobody”用户的身份执行操作系统命令。

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-2021-0004

5. Google Chrome 缓冲区错误漏洞（CNNVD-202103-268）

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

Google Chrome 存在安全漏洞，该漏洞源于 V8 中的越界内存访问，允许远程攻击者通过精心制作的 HTML 页面执行越界内存访问。

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/2021/03/stable-channel-upda

te-for-desktop.html

6. Microsoft Visual Studio 后置链接漏洞（CNNVD-202103-640）

Microsoft Visual Studio 是美国微软（Microsoft）公司的一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。Git for Visual Studio 是其中的一个 Git（分布式版本控制系统）扩展。

Git for Visual Studio 存在安全漏洞。以下产品和版本受到影响：Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8),Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3),Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6),Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8),Microsoft Visual Studio 2019 version 16.8 (includes 16.0 - 16.7)。

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-2021-21300

7. Linux kernel 资源管理错误漏洞（CNNVD-202103-1576）

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。

Linux kernel before 5.11.9 存在资源管理错误漏洞，该漏洞源于 drivers/vhost/vdpa.c 重新打开字符设备时有一个无效的值。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commi

t/?id=f6bbf0010ba004f5e90c7aefdebc0ee4bd3283b9

8. Adobe Creative Cloud Desktop Application 输入验证错误漏洞（CNNVD-202103-792）

Adobe Creative Cloud Desktop Application 是美国奥多比（Adobe）公司的一套用于在 Creative 云会员管理中心管理应用程序和服务的应用程序。该程序支持同步和共享文件、管理字体以及访问商业摄影和设计的资产库。

Adobe Creative Cloud Desktop Application 11.0.5 存在输入验证错误漏洞，攻击者可以利用此漏洞窃取受害者基于 cookie 的身份验证凭据。

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/creative-cloud/apsb21-18.html

二、接报漏洞情况

本月接报漏洞 11186 个，其中信息技术产品漏洞（通用型漏洞）100 个，网络信息系统漏洞（事件型漏洞）11086 个。

表 7 2021 年 3 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	8025
2	上海斗象信息科技有限公司	1305
3	北京山石网科信息技术有限公司	382
4	北京华云安信息技术有限公司	164

5	北京天地和兴科技有限公司	138
6	微步在线科技有限公司	130
7	山东华鲁科技发展股份有限公司	106
8	南京众智维信息科技有限公司	102
9	太极计算机股份有限公司	65
10	杭州海康威视数字技术股份有限公司	58
11	北京数字观星科技有限公司	50
12	安徽长泰信息安全服务有限公司	46
13	内蒙古奥创科技有限公司	44
14	北京顶象技术有限公司 洞见安全实验室	39
15	北京优炫软件股份有限公司	37
16	山东云天安全技术有限公司	35
17	西安交大捷普网络科技有限公司	30
18	北京奇虎科技有限公司	27
19	内蒙古思沃科技有限公司	26
20	内蒙古洞明科技有限公司	25
21	安徽华云网安信息技术有限公司	22
22	北京赋云安运营科技有限公司	21
23	广州锦行网络科技有限公司	21
24	西安四叶草信息技术有限公司	20
25	星云博创摘星实验室	20
26	远江盛邦（北京）网络安全科技股份有限公司	20
27	北京启明星辰信息安全技术有限公司	19

28	北京安帝科技有限公司	16
29	北京云测信息技术有限公司	16
30	广州竞远安全技术股份有限公司	16
31	北京安全共识科技有限公司	15
32	北京威努特技术有限公司	14
33	杭州默安科技有限公司	11
34	北京机沃科技有限公司	10
35	北京圣博润高新技术股份有限公司	9
36	上海谋乐网络科技有限公司	9
37	上海银基信息安全技术有限公司	8
38	中兴通讯	8
39	群智自動化機械有限公司	7
40	任子行网络技术股份有限公司	7
41	中国电信集团系统集成有限责任公司	7
42	北京国舜科技股份有限公司	6
43	北京天融信网络安全技术有限公司	6
44	中通服咨询设计研究院有限公司	6
45	博智安全科技股份有限公司	5
46	个人	5
47	中电长城网际系统应用有限公司	5
48	北京智游网安科技有限公司	4
49	北京知道创宇信息技术股份有限公司	3
50	海南神州希望网络有限公司	2

51	江苏金盾检测技术有限公司	2
52	上海大学	2
53	上海天民信息技术有限公司	2
54	广州天懋信息系统股份有限公司	1
55	华为技术有限公司未然实验室	1
56	北京墨云科技有限公司	1
57	江苏天创科技有限公司	1
58	山东道普测评技术有限公司安徽分公司	1
59	上海三零卫士信息安全有限公司	1
60	上海上讯信息技术股份有限公司	1
61	深圳市魔方安全科技有限公司	1
报送总计		6087

三、重大漏洞预警

3.1 F5 BIG-IP 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 F5 BIG-IP 安全漏洞（CNNVD-202007-053、CVE-2020-5902）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 15.1.0 版本，15.0.0 版本，14.1.0 版本至 14.1.2 版本，13.1.0 版本至 13.1.3 版本，12.1.0 版本至 12.1.5 版本，11.6.1 版本至 11.6.5 版本等多个版本均受此漏洞影响。目前，F5 官方已经发布了修复漏洞的升级版本，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 中存在安全漏洞。攻击者可在未授权的情况下，向漏洞页面发送特制的请求包，从而远程执行命令、创建或删除文件，开启或关闭服务等操作。

. 危害影响

F5 BIG-IP 15.1.0 版本，15.0.0 版本，14.1.0 版本至 14.1.2 版本，13.1.0 版本至 13.1.3 版本，12.1.0 版本至 12.1.5 版本，11.6.1 版本至 11.6.5 版本等多个版本均受此漏洞影响。

. 修复建议

目前，F5 官方已经发布了修复漏洞的升级版本，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。版本升级措施如下：

BIG-IP 15.x: 15.1.0.4

BIG-IP 14.x: 14.1.2.6

BIG-IP 13.x: 13.1.3.4

BIG-IP 12.x: 12.1.5.2

BIG-IP 11.x: 11.6.5.2

官方升级地址如下：

https://support.f5.com/csp/article/K52145254

3.2 Microsoft Exchange 多个安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Microsoft Exchange 多个安全漏洞情况的报送，其中包括 Microsoft Exchange 安全漏洞（CNNVD-202103-192、CVE-2021-26855）、Microsoft Exchange 安全漏洞（CNNVD-202103-191、CVE-2021-26857）等多个安全漏洞。成功利用漏洞的攻击者可以在目标系统中获取敏感信息、写入任意文件、执行恶意代码等。Microsoft Exchange 2010、Microsoft Exchange 2013、Microsoft Exchange 2016、Microsoft Exchange 2019 等版本均受漏洞影响。目前，微软官方已发布补丁修复了上述漏洞，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 Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。

1、Microsoft Exchange 安全漏洞（CNNVD-202103-192、CVE-2021-26855）：

攻击者可构造恶意 HTTP 请求，并通过 Exchange Server 进行身份验证。进而扫描内网，获取用户敏感信息。

2、Microsoft Exchange 安全漏洞（CNNVD-202103-191、CVE-2021-26857）：

攻击者可构造恶意请求，触发反序列化漏洞，从而执行任意代码。

成功利用该漏洞需要 Exchange 管理员权限，或需要配合其他漏洞使用。

3、Microsoft Exchange 安全漏洞（CNNVD-202103-189、CVE-2021-26858）（CNNVD-202103-188、CVE-2021-27065）：

攻击者通过 Exchange 服务器进行身份验证后，可以利用此漏洞将文件写入服务器上的任何路径。

.危害影响

成功利用漏洞的攻击者可以在目标系统中获取敏感信息、写入任意文件、执行恶意代码等。Microsoft Exchange 2010、Microsoft Exchange 2013、Microsoft Exchange 2016、Microsoft Exchange 2019 等版本均受漏洞影响。

.修复建议

目前，微软官方已发布补丁修复了上述漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26857

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26858

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27065