信息安全漏洞通报

2020 年 8 月 **国家信息安全漏洞库（CNNVD）**

本 期 导 读

漏洞态势

根据国家信息安全漏洞库（CNNVD）统计，2020 年 8 月份采集安全漏洞共 1284 个。

本月接报漏洞 10500 个，其中信息技术产品漏洞（通用型漏洞）61 个，网络信息系统漏洞（事件型漏洞）10499 个。

重大漏洞预警

宝塔服务器运维面板权限许可和访问控制漏洞（CNNVD-202008-1141）：成功利用漏洞的攻击者可以在无需管理员授权的情况下进入数据库修改或删除数据。宝塔面板 Linux 版 7.4.2 版、宝塔面板 Linux 版 7.5.14 测试版、宝塔面板 Windows 版 6.8 版均受此漏洞影响。目前，宝塔服务器运维面板官方已经发布了补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

Apache Struts2 S2-059 安全漏洞（CNNVD-202008-743、CVE-2019-0230）：成功利用漏洞的攻击者可能对目标系统执行恶意代码。Apache Struts 2.0.0–Apache Struts 2.5.20 等版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，及时采取修补措施。

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 8 月份新增安全漏洞共 1284 个，从厂商分布来看，Microsoft 公司产品的漏洞数量最多，共发布 121 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 13.47%。本月新增漏洞中，超危漏洞 110 个、高危漏洞 509 个、中危漏洞 631 个、低危漏洞 34 个，相应修复率分别为 82.73%、88.80%、77.02%以及 85.29%。合计 1058 个漏洞已有修复补丁发布，本月整体修复率 82.40%。

截至 2020 年 08 月 31 日，CNNVD 采集漏洞总量已达 149895 个。

1.1 漏洞增长概况

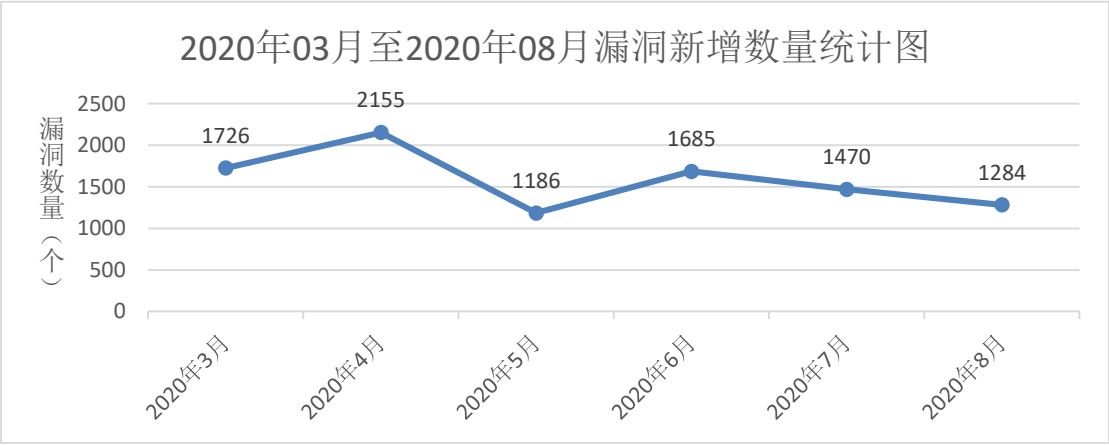

图 1 2020 年 3 月至 2020 年 8 月漏洞新增数量统计图

2020 年 8 月新增安全漏洞 1284 个，与上月（1470 个）相比减少了 12.65%。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 1584 个。

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

8 月厂商漏洞数量分布情况如表 1 所示，Microsoft 公司漏洞达到 121 个，占本月漏洞总量的 9.42%。

表 1　2020 年 8 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	Microsoft	121	9.42%
2	Google	69	5.37%
3	IBM	58	4.52%
4	Cisco	58	4.52%
5	Intel	51	3.97%
6	Qualcomm	49	3.82%
7	Adobe	33	2.57%
8	Artifex Software	26	2.02%
9	Huawei	24	1.87%
10	Git	18	1.40%

1.2.2 漏洞产品分布

8 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 88 个，其中 Windows 10 漏洞数量最多，共 86 个，占主流操作系统漏洞总量的 14.80%，排名第一。

表 2　2020 年 8 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	86
2	Windows Server 2019	70

3	Windows Server 2016	63
4	Windows 8.1	56
5	Windows Rt 8.1	55
6	Windows 7	52
7	Windows Server 2012	46
8	Windows Server 2012 R2	46
9	Windows Server 2008	41
10	Windows Server 2008 R2	41
11	Android	23
12	Linux Kernel	2

*由于 Windows 整体市占率高达百分之九十以上，所以上表针对不同的 Windows 版本分别进行统计

*上表漏洞数量为影响该版本的漏洞数量，由于同一漏洞可能影响多个版本操作系统，计算某一系列操作系统漏洞总量时，不能对该系列所有操作系统漏洞数量进行简单相加。

1.2.3 漏洞类型分布

8 月份发布的漏洞类型分布如表 3 所示，其中缓冲区错误类漏洞所占比例最大，约为 13.47%。

表 3 2020 年 8 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	173	13.47%
2	跨站脚本	128	9.97%
3	输入验证错误	112	8.72%
4	信息泄露	71	5.53%
5	代码问题	51	3.97%
6	SQL 注入	46	3.58%
7	授权问题	46	3.58%
8	资源管理错误	45	3.50%
9	路径遍历	31	2.41%
10	操作系统命令注入	23	1.79%
11	访问控制错误	21	1.64%
12	跨站请求伪造	16	1.25%
13	注入	15	1.17%
14	信任管理问题	13	1.01%
15	加密问题	9	0.70%

16	代码注入	6	0.47%
17	数据伪造问题	5	0.39%
18	竞争条件问题	5	0.39%
19	数字错误	4	0.31%
20	后置链接	3	0.23%
21	权限许可和访问控制问题	2	0.16%
22	命令注入	2	0.16%
23	环境问题	2	0.16%
24	参数注入	2	0.16%
25	日志信息泄露	1	0.08%
26	安全特征问题	1	0.08%
27	格式化字符串错误	1	0.08%
28	配置错误	1	0.08%
29	其他	415	32.32%

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。8 月漏洞危害等级分布如图 2 所示，其中超危漏洞 110 条，占本月漏洞总数的 8.57%。

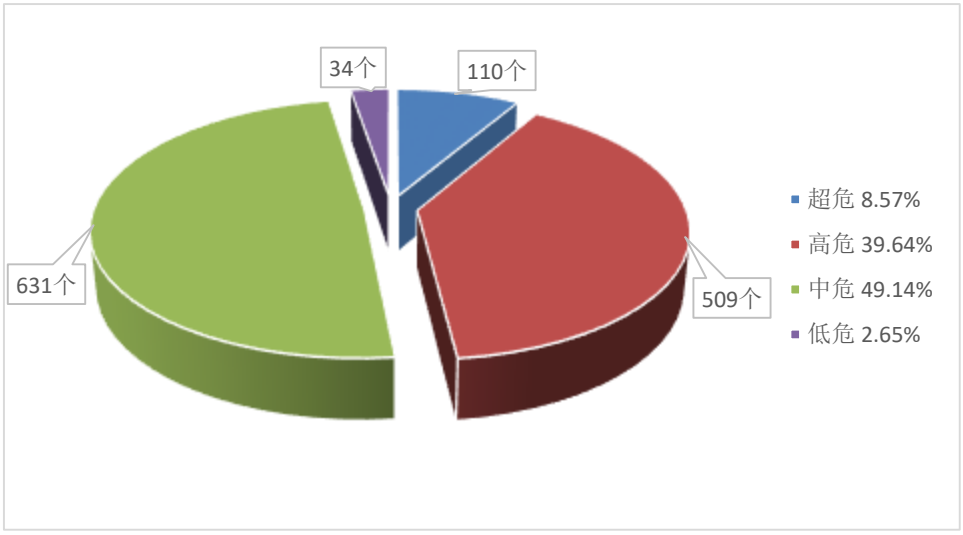

图 2　2020 年 8 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

8 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 88.80%，中危漏洞修复率最低，比例为 77.02%。总体来看，本月整体修复率，由上月的 83.98%下降至本月的 82.40%。

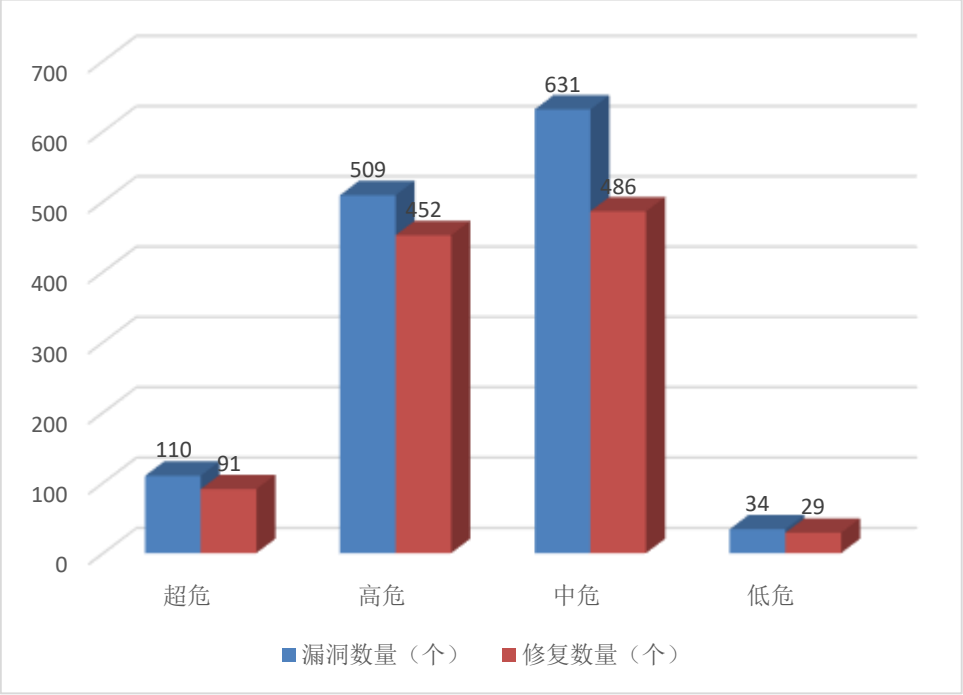

图 3　2020 年 8 月漏洞修复数量统计

1.3.2 厂商修复情况

8 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Microsoft、Google、IBM 等十个厂商共 507 条漏洞，占本月漏洞总数的 39.49%，漏洞修复率为 98.22%，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 Microsoft、Google、IBM、Qualcomm、Adobe、Artifex Software、Huawei 等公司本月漏洞修复率均为 100%，共 498 条漏洞已全部修复。

表 4　2020 年 8 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	Microsoft	121	121	100.00%
2	Google	69	69	100.00%
3	IBM	58	58	100.00%
4	Cisco	58	51	87.93%
5	Intel	51	50	98.04%
6	Qualcomm	49	49	100.00%
7	Adobe	33	33	100.00%
8	Artifex Software	26	26	100.00%
9	Huawei	24	24	100.00%
10	Git	18	17	94.44%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

本月超危漏洞共 110 个，其中重要漏洞实例如表 5 所示。

表 5　2020 年 8 月超危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202008-1340	13ENFORME	Apache SkyWalking SQL注入漏洞（CNNVD-202008-152）
		CNNVD-202008-152	Apache 软件基金会	
		CNNVD-202008-678	Citrix Systems	
		CNNVD-202008-851	DBSoft	
		CNNVD-202008-1503	Open Solutions for Education	
		CNNVD-202008-1504		
		CNNVD-202008-1505		
		CNNVD-202008-1506		
		CNNVD-202008-1513		
		CNNVD-202008-1338	Solidus 项目	
		CNNVD-202008-669	thedaylightstudio	
		CNNVD-202008-861	个人开发者	
2	操作系统命令注入	CNNVD-202008-150	Aerospike	Aerospike 操作系统命令注入漏洞（CNNVD-202008-150）
		CNNVD-202008-276	Firejail 项目	
		CNNVD-202008-1095	Moog	
		CNNVD-202008-095	Red Hat	
3	代码问题	CNNVD-202008-871	Autovance Technologies	WordPress 中 wpDiscuz 插件安全漏洞
		CNNVD-202008-1218	Rackspace	

		CNNVD-202008-1075	UNIFI	（CNNVD-202008-1145）
		CNNVD-202008-1145	WordPress	
		CNNVD-202008-842	ZKTeco	
4	缓冲区错误	CNNVD-202008-281	Apache 软件基金会	Apache HTTP Server 缓冲区错误漏洞（CNNVD-202008-281）
		CNNVD-202008-049	Google	
		CNNVD-202008-688		
		CNNVD-202008-258	Ivanti	
		CNNVD-202008-120	NETGEAR	
		CNNVD-202008-011	Qualcomm	
		CNNVD-202008-038		
		CNNVD-202008-040		
		CNNVD-202008-674	个人开发者	
		CNNVD-202008-1091		
5	跨站脚本	CNNVD-202008-1371	redlion	Marvell QConvergeConsole 安全漏洞（CNNVD-202008-349）
		CNNVD-202008-1374		
		CNNVD-202008-454	SAP	
		CNNVD-202008-578	Siemens	
		CNNVD-202008-1197	advantech	
		CNNVD-202008-349	Marvell	
		CNNVD-202008-1527	Open Solutions for Education	
		CNNVD-202008-594	Schneider Electric	
		CNNVD-202008-596		
		CNNVD-202008-299	SecurEnvoy	
		CNNVD-202008-164	Yokogawa	
6	其他	CNNVD-202008-691	Citrix Systems	Microsoft Windows NetLogon 安全漏洞（CNNVD-202008-548）
		CNNVD-202008-992	Design Create Play 团队	
		CNNVD-202008-1417	google	
		CNNVD-202008-1482		
		CNNVD-202008-1484		
		CNNVD-202008-1488		
		CNNVD-202008-1494		
		CNNVD-202008-1202	gradle	
		CNNVD-202008-161	LilyPond 项目	
		CNNVD-202008-1448	manageengine	
		CNNVD-202008-548	Microsoft	
		CNNVD-202008-1278	mitel	
		CNNVD-202008-1097	Moog	
		CNNVD-202008-1499	openSIS	
		CNNVD-202008-1500		
		CNNVD-202008-616	Pivotal Software	

		CNNVD-202008-1367	redlion	
		CNNVD-202008-1142	squid-cache	
		CNNVD-202008-278	SUSE	
		CNNVD-202008-1086	wso2	
		CNNVD-202008-1088		
		CNNVD-202008-370	ZOHO	
		CNNVD-202008-1143	个人开发者	
		CNNVD-202008-1280		
		CNNVD-202008-1471		
7	输入验证错误	CNNVD-202008-656	BlackBerry	Json Pattern Validator 输入验证错误漏洞（CNNVD-202008-384）
		CNNVD-202008-384	Json Pattern Validator 项目	
		CNNVD-202008-073	Key Vault	
		CNNVD-202008-041	Qualcomm	
		CNNVD-202008-074		
		CNNVD-202008-081		
		CNNVD-202008-090		
		CNNVD-202008-093		
		CNNVD-202008-098		
		CNNVD-202008-866	个人开发者	
		CNNVD-202008-922		
		CNNVD-202008-924		
		CNNVD-202008-929		
8	信任管理问题	CNNVD-202008-954	Cisco	Cisco ENCS 5400-W Series 和 CSP 5000-W Series 信任管理问题漏洞（CNNVD-202008-954）
		CNNVD-202008-085	IBM	
		CNNVD-202008-1291		
		CNNVD-202008-260	Ivanti	
		CNNVD-202008-602	Roboteam Home	
		CNNVD-202008-1254	个人开发者	

1. Apache SkyWalking SQL 注入漏洞（CNNVD-202008-152）

Apache SkyWalking 是美国阿帕奇软件（Apache Software）基金会的一款主要用于微服务、云原生和基于容器等环境的应用程序性能监视器。

Apache SkyWalking（H2/MySQL/TiDB 存储选项被激活）中存在 SQL 注入漏洞。攻击者可通过构建通配符查询语句利用该漏洞获取用

户的数据库敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/r6f3a934ebc54585d8468151a494c1919dc1ee2cccaf237ec434dbbd6@%3Cdev.skywalking.apache.org%3E

2. Aerospike 操作系统命令注入漏洞（CNNVD-202008-150）

Aerospike 是美国 Aerospike 公司的一套 NoSQL 数据库解决方案。

Aerospike（社区版）4.9.0.5 版本中存在安全漏洞。攻击者借助特制的 UDF 利用该漏洞以当前用户权限在该集群的所有节点上执行任意的操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.aerospike.com/enterprise/download/server/notes.html#5.1.0.3

3. WordPress 中 wpDiscuz 插件安全漏洞（CNNVD-202008-1145）

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 wpDiscuz 7.0.4 之前版本中存在远程代码执行漏洞，该漏洞允许攻击者上传任意文件。.

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://blog.zulip.com/2020/06/17/zulip-server-2-1-5-security-release/

4. **Apache HTTP Server 缓冲区错误漏洞（CNNVD-202008-281）**

Apache HTTP Server 是美国阿帕奇软件（Apache Software）基金

会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API 进行扩充的特点。

Apache HTTP Server 2.4.32 版本至 2.4.44 版本中的 mod_uwsgi 存在缓冲区错误漏洞。攻击者可利用该漏洞获取信息并可能执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2020-9490

5. Marvell QConvergeConsole 安全漏洞（CNNVD-202008-349）

Marvell QConvergeConsole（QCC）是美国美满科技（Marvell）公司的一款跨数据中心的统一适配器管理软件。该软件主要用于以太网和光纤通道适配器管理等。

Marvell QConvergeConsole 5.5.0.64 版本中存在安全漏洞。该漏洞允许攻击者远程执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.marvell.com/content/dam/marvell/en/public-collateral/fibre-channel/marvell-fibre-channel-security-advisory-2020-07.pdf

6. Microsoft Windows NetLogon 安全漏洞（CNNVD-202008-548）

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Netlogon 是一个用于为域控制器注册所有 SRV 资源记录的服务。

Microsoft Windows NetLogon 中存在提权漏洞。攻击者可借助特

制应用程序利用该漏洞获取管理员访问权限。以下产品及版本受到影响：Microsoft Windows Server 2008 R2 SP1，Windows Server 2012，Windows Server 2012 R2，Windows Server 2016，Windows Server 2019，Windows Server 1903 版本，Windows Server 1909 版本，Windows Server 2004 版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1472

7. Json Pattern Validator 输入验证错误漏洞（CNNVD-202008-384）

Json Pattern Validator（JPV）是一款 JSON 模式验证器。

JPV 2.2.2 之前版本中存在安全漏洞，该漏洞源于程序没有正确验证输入。攻击者可利用该漏洞绕过验证。

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/manvel-khnkoyan/jpv/commit/e3eec1215caa8d5c560f5e88d0943422831927d6

8. Cisco ENCS 5400-W Series 和 CSP 5000-W Series 信任管理问题漏洞（CNNVD-202008-954）

Cisco Enterprise NFV Infrastructure Software（NFVIS）是美国思科（Cisco）公司的一套 NVF 基础架构软件平台。该平台可以通过中央协调器和控制器实现虚拟化服务的全生命周期管理。

Cisco ENCS 5400-W Series 和 CSP 5000-W Series 中的 Virtual Wide Area Application Services (vWAAS)（带有 NFVIS 捆绑的镜像）

存在信任管理问题漏洞，该漏洞源于用户账户使用了默认的静态密码。攻击者可借助该漏洞利用该漏洞登录到 NFVIS CLI 中。

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-waas-encsw-cspw-cred-hZzL29A7

1.4.2 高危漏洞实例

本月高危漏洞共 509 个，其中重点漏洞实例如表 6 所示。

表 6　2020 年 8 月高危漏洞实例

序号	漏洞类型	CNNVD 编号	厂商	漏洞实例
1	SQL 注入	CNNVD-202008-399	Carson & SAINT	Carson＆SAINT SAINT Security Suite SQL 注入漏洞（CNNVD-202008-399）
		CNNVD-202008-401		
		CNNVD-202008-125	ERPNext	
		CNNVD-202008-746	Loway	
		CNNVD-202008-748		
		CNNVD-202008-1411	riken	
2	操作系统命令注入	CNNVD-202008-1186	cellosoft	Sophos XG Firewall 操作系统命令注入漏洞（CNNVD-202008-303）
		CNNVD-202008-107	Cohesive Networks 团队	
		CNNVD-202008-275	Firejail 项目	
		CNNVD-202008-267	Geutebrück	
		CNNVD-202008-697	Huawei	
		CNNVD-202008-1297	ibm	
		CNNVD-202008-854	NoviFlow	
		CNNVD-202008-563	SABnzbd	
		CNNVD-202008-303	Sophos	
		CNNVD-202008-859	Ubiquiti Networks	
		CNNVD-202008-180	个人开发者	
		CNNVD-202008-1092		
		CNNVD-202008-1176		
3	代码问题	CNNVD-202008-166	Cisco	Cisco FXOS Software 和 Cisco NX-OS Software 安全漏洞
		CNNVD-202008-1311		
		CNNVD-202008-1195	fasterxml	

		CNNVD-202008-328	flatCore	（CNNVD-202008-1311）
		CNNVD-202008-1139	github	
		CNNVD-202008-346		
		CNNVD-202008-347		
		CNNVD-202008-129	IBM	
		CNNVD-202008-737	Intel	
		CNNVD-202008-316	JetBrains	
		CNNVD-202008-982	Linux 基金会	
		CNNVD-202008-864	Lua 团队	
		CNNVD-202008-379	Marvell	
		CNNVD-202008-764	Philips	
		CNNVD-202008-749	PostgreSQL 组织	
		CNNVD-202008-750		
		CNNVD-202008-013	Qualcomm	
		CNNVD-202008-036		
		CNNVD-202008-829	Rapid Software	
		CNNVD-202008-086	Red Hat	
		CNNVD-202008-088	Teltonika	
		CNNVD-202008-092		
		CNNVD-202008-1079	Tenable Network Security 机构	
		CNNVD-202008-574	Teradici	
		CNNVD-202008-836	Zoom	
4	访问控制错误	CNNVD-202008-843	Beijing Kuangshi Technology	多款 Qualcomm 产品访问控制错误漏洞（CNNVD-202008-022）
		CNNVD-202008-342	GitLab	
		CNNVD-202008-343		
		CNNVD-202008-1023	NCR	
		CNNVD-202008-181	projectcontour	
		CNNVD-202008-022	Qualcomm	
		CNNVD-202008-058		
5	缓冲区错误	CNNVD-202008-126	ACTi	Microsoft Excel 缓冲区错误漏洞（CNNVD-202008-434）
		CNNVD-202008-410	Adobe	
		CNNVD-202008-411		
		CNNVD-202008-412		
		CNNVD-202008-414		
		CNNVD-202008-416		
		CNNVD-202008-419		
		CNNVD-202008-422		
		CNNVD-202008-424		
		CNNVD-202008-437		
		CNNVD-202008-439		

		CNNVD-202008-440		
		CNNVD-202008-261	Advantech	
		CNNVD-202008-265		
		CNNVD-202008-266		
		CNNVD-202008-141	Cisco	
		CNNVD-202008-1307		
		CNNVD-202008-935	Corel	
		CNNVD-202008-118	Delta Electronics	
		CNNVD-202008-124		
		CNNVD-202008-253		
		CNNVD-202008-259		
		CNNVD-202008-262		
		CNNVD-202008-264		
		CNNVD-202008-650	Dovecot	
		CNNVD-202008-652		
		CNNVD-202008-1163	drbenhur	
		CNNVD-202008-1201	foxit	
		CNNVD-202008-1203		
		CNNVD-202008-047	Google	
		CNNVD-202008-048		
		CNNVD-202008-383		
		CNNVD-202008-952		
		CNNVD-202008-110	HumanTalk	
		CNNVD-202008-1161	ibm	
		CNNVD-202008-591	Intel	
		CNNVD-202008-597		
		CNNVD-202008-601		
		CNNVD-202008-617		
		CNNVD-202008-618		
		CNNVD-202008-623		
		CNNVD-202008-629		
		CNNVD-202008-420	Microsoft	
		CNNVD-202008-421		
		CNNVD-202008-423		
		CNNVD-202008-425		
		CNNVD-202008-428		
		CNNVD-202008-431		
		CNNVD-202008-434		
		CNNVD-202008-436		
		CNNVD-202008-456		
		CNNVD-202008-457		
		CNNVD-202008-459		

		CNNVD-202008-469		
		CNNVD-202008-472		
		CNNVD-202008-478		
		CNNVD-202008-480		
		CNNVD-202008-481		
		CNNVD-202008-482		
		CNNVD-202008-483		
		CNNVD-202008-484		
		CNNVD-202008-485		
		CNNVD-202008-486		
		CNNVD-202008-487		
		CNNVD-202008-488		
		CNNVD-202008-489		
		CNNVD-202008-490		
		CNNVD-202008-500		
		CNNVD-202008-502		
		CNNVD-202008-508		
		CNNVD-202008-115	NETGEAR	
		CNNVD-202008-006	Qualcomm	
		CNNVD-202008-007		
		CNNVD-202008-008		
		CNNVD-202008-012		
		CNNVD-202008-020		
		CNNVD-202008-021		
		CNNVD-202008-026		
		CNNVD-202008-035		
		CNNVD-202008-042		
		CNNVD-202008-055		
		CNNVD-202008-685	Scanpoint Software	
6	授权问题	CNNVD-202008-870	Apache 软件基金会	Apache Shiro 安全漏洞（CNNVD-202008-870）
		CNNVD-202008-304	Assmann Electronic	
		CNNVD-202008-045	Bitdefender	
		CNNVD-202008-1304	cisco	
		CNNVD-202008-672	Huawei	
		CNNVD-202008-744	IBM	
		CNNVD-202008-619	Intel	
		CNNVD-202008-620		
		CNNVD-202008-624		
		CNNVD-202008-625		

		CNNVD-202008-296	Lindy	
		CNNVD-202008-1415	mediawiki	
		CNNVD-202008-1018	NCR	
		CNNVD-202008-408	SAP	
		CNNVD-202008-583	Siemens	
		CNNVD-202008-292	TP-Link	
7	输入验证错误	CNNVD-202008-850	Apache 软件基金会	Microsoft Internet Explorer 安全漏洞（CNNVD-202008-4270）
		CNNVD-202008-170	Cisco	
		CNNVD-202008-178		
		CNNVD-202008-957		
		CNNVD-202008-958		
		CNNVD-202008-965		
		CNNVD-202008-1296		
		CNNVD-202008-1299		
		CNNVD-202008-1301		
		CNNVD-202008-932	Corel	
		CNNVD-202008-941		
		CNNVD-202008-944		
		CNNVD-202008-252	Delta Electronics	
		CNNVD-202008-1219	f5	
		CNNVD-202008-1228		
		CNNVD-202008-103	Google	
		CNNVD-202008-1487		
		CNNVD-202008-1493		
		CNNVD-202008-1021	HashiCorp	
		CNNVD-202008-111	HumanTalk	
		CNNVD-202008-614	Intel	
		CNNVD-202008-632		
		CNNVD-202008-640		
		CNNVD-202008-1078	ISC	
		CNNVD-202008-183	McAfee	
		CNNVD-202008-427	Microsoft	
		CNNVD-202008-476		
		CNNVD-202008-550		
		CNNVD-202008-016	Qualcomm	
		CNNVD-202008-023		
		CNNVD-202008-029		
		CNNVD-202008-030		
		CNNVD-202008-032		
		CNNVD-202008-033		
		CNNVD-202008-034		

		CNNVD-202008-044		
		CNNVD-202008-053		
		CNNVD-202008-062		
		CNNVD-202008-122	SoftPerfect	
		CNNVD-202008-1103	wolfssl	
8	资源管理错误	CNNVD-202008-438	Adobe	Cisco IOS 和 Cisco IOS XR 资源管理错误漏洞（CNNVD-202008-1423）
		CNNVD-202008-446		
		CNNVD-202008-268	Advantech	
		CNNVD-202008-718	Artifex Software	
		CNNVD-202008-1423	cisco	
		CNNVD-202008-109	Foxit	
		CNNVD-202008-070	Google	
		CNNVD-202008-072		
		CNNVD-202008-076		
		CNNVD-202008-373		
		CNNVD-202008-374		
		CNNVD-202008-376		
		CNNVD-202008-377		
		CNNVD-202008-381		
		CNNVD-202008-389		
		CNNVD-202008-393		
		CNNVD-202008-395		
		CNNVD-202008-397		
		CNNVD-202008-1178		
		CNNVD-202008-824	ISE	
		CNNVD-202008-271	Linux 基金会	
		CNNVD-202008-759	NGINX	
		CNNVD-202008-004	Qualcomm	
		CNNVD-202008-015		
		CNNVD-202008-028		
		CNNVD-202008-951	Red Hat	

1. Carson＆SAINT SAINT Security Suite SQL 注入漏洞（CNNVD-202008-399）

Carson＆SAINT SAINT Security Suite 是美国 Carson＆SAINT 公司的一套提供漏洞管理、安全配置评估、渗透测试等功能的安全套件。

Carson＆SAINT SAINT Security Suite 8.0 版本至 9.8.20 版本中的 Assets 组件存在 SQL 注入漏洞。远程攻击者可利用该漏洞未授权访问数据库。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://download.saintcorporation.com/products/saint_advisory15.txt

2. Sophos XG Firewall 操作系统命令注入漏洞

（CNNVD-202008-303）

Sophos XG Firewall 是英国 Sophos 公司的一款下一代端点保护与企业级防火墙产品。

Sophos XG Firewall 2020-08-05 及之前版本中的 User Portal 存在操作系统命令注入漏洞。该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令等。攻击者可利用该漏洞执行非法操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://community.sophos.com/b/security-blog/posts/advisory-resolved-authenticated-rce-issues-in-user-portal-cve-2020-17352

3. Cisco FXOS Software 和 Cisco NX-OS Software 安全漏洞

（CNNVD-202008-1311）

Cisco NX-OS Software 和 Cisco FXOS Software 都是美国思科（Cisco）公司的产品。Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。Cisco FXOS Software 是一套运行在思科安全设备中的防火墙软件。

Cisco FXOS Software 和 Cisco NX-OS Software 中的 Fabric 服务组件存在安全漏洞，该漏洞源于受影响的软件分析 Cisco 结构服务消息时错误处理不足，攻击者可以利用该漏洞导致拒绝服务攻击。

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.cisco.com/

4. 多款 Qualcomm 产品访问控制错误漏洞（CNNVD-202008-022）

Qualcomm SDA660 等都是美国高通（Qualcomm）公司的一款中央处理器（CPU）产品。

多款 Qualcomm 产品中的 Core 存在访问控制错误漏洞。该漏洞源于网络系统或产品未正确限制来自未授权角色的资源访问。以下产品及版本受到影响：Qualcomm APQ8098；Kamorta；MSM8998；QCS404；QCS605；SDA660；SDA845；SDM630；SDM636；SDM660；SDM670；SDM710；SDM845；SDM850；SXR1130。

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/august-2020-security-bulletin

5. Microsoft Excel 缓冲区错误漏洞（CNNVD-202008-434）

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 Excel 中存在远程代码执行漏洞，该漏洞源于程序没有正确处理内存中的对象。攻击者可借助特制文件利用该漏洞在当前用户上下文中运行任意代码。以下产品及版本受到影响：Microsoft Ex

cel 2010 SP2，Excel 2013 RT SP1，Excel 2013 SP1，Excel 2016；Office 2016 for Mac， Office 2019，Office 2019 for Mac，365 Apps for Enterprise。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1498

6. Apache Shiro 安全漏洞（CNNVD-202008-870）

Apache Shiro 是美国阿帕奇（Apache）软件基金会的一套用于执行认证、授权、加密和会话管理的 Java 安全框架。

Apache Shiro 1.6.0 之前版本中存在安全漏洞。攻击者可借助特制的 HTTP 请求利用该漏洞绕过身份验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread.html/r539f87706094e79c5da0826030384373f00410689369128768568 35f%40%3Cdev.shiro.apache.org%3E

7. Microsoft Internet Explorer 安全漏洞（CNNVD-202008-427）

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。

Microsoft IE 9 版本和 11 版本中的 MSHTML Engine 存在远程代码执行漏洞，该漏洞源于程序没有正确验证输入。攻击者可借助特制文件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://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory

/CVE-2020-1567

8. Cisco IOS 和 Cisco IOS XR 资源管理错误漏洞

（CNNVD-202008-1423）

Cisco IOS 和 Cisco IOS XR 都是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。

Cisco IOS XR Software 中的 DVMRP 存在安全漏洞，该漏洞源于 Internet 组管理协议（IGMP）数据包的队列管理不足造成的，攻击者可以通过向受影响的设备发送精心编制的 IGMP 数据包来进行攻击。

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-iosxr-dvmrp-memexh-dSmpdvfz

二、接报漏洞情况

本月接报漏洞 10500 个，其中信息技术产品漏洞（通用型漏洞）61 个，网络信息系统漏洞（事件型漏洞）10499 个。

表 7 2020 年 7 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	5298
2	上海斗象信息科技有限公司	4244
3	内蒙古奥创科技	220
4	长春嘉诚信息技术股份有限公司	140
5	北京华云安信息技术有限公司	137

6	西安四叶草信息技术有限公司	60
7	山东新潮信息技术有限公司	55
8	北京顶象技术有限公司 洞见安全实验室	37
9	北京天地和兴科技有限公司	36
10	北京梆梆安全科技有限公司	33
11	北京数字观星科技有限公司	24
12	广州锦行网络科技有限公司	20
13	远江盛邦（北京）网络安全科技股份有限公司	20
14	上海市信息安全测评中心	18
15	北京天融信网络安全技术有限公司	16
16	绿盟科技集团股份有限公司	12
17	山东泽鹿安全技术有限公司	10
18	星云博创科技有限公司	10
19	太极计算机股份有限公司	10
20	新华三技术有限公司	10
21	湖南匡安网络技术有限公司	9
22	安徽长泰信息安全服务有限公司	7
23	绿盟科技集团股份有限公司	7
24	中国电子科技网络信息安全有限公司	7
25	北京安帝科技有限公司	6
26	北京安信天行科技有限公司	5
27	上海银基信息安全技术股份有限公司	5
28	安全邦（北京）信息技术有限公司	4

29	WRLab	4
30	个人	3
31	北京智游网安科技有限公司	3
32	上海安识网络科技有限公司	3
33	北京长亭科技有限公司	3
34	安徽锋刃信息科技有限公司	2
35	杭州默安科技有限公司	2
36	内蒙古洞明科技有限公司	2
37	上海大学机电工程与自动化学院	2
38	深圳市魔方安全科技有限公司	2
39	中兴通讯	2
40	北京启明星辰信息安全技术有限公司	1
41	北京智游网安科技有限公司	1
42	北京华圣龙源科技有限公司	1
43	国网山西省电力公司电力科学研究院	1
44	杭州木链物联网科技有限公司	1
45	恒安嘉新（北京）科技股份公司	1
46	湖南网鼎科技有限公司	1
47	华为技术有限公司	1
48	江西神舟信息安全评估中心有限公司	1
49	信息工程大学	1
50	重庆梦之想科技有限责任公司	1
51	北京奇虎科技有限公司	1

报送总计	10500

三、重大漏洞预警

3.1 宝塔服务器运维面板权限许可和访问控制漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于宝塔服务器运维面板权限许可和访问控制漏洞（CNNVD-202008-1141）情况的报送。成功利用漏洞的攻击者可以在无需管理员授权的情况下进入数据库修改或删除数据，并且可以通过互联网远程访问管理页面，获取服务器系统权限，最终控制目标服务器。宝塔面板 Linux 版 7.4.2 版、宝塔面板 Linux 版 7.5.14 测试版、宝塔面板 Windows 版 6.8 版均受此漏洞影响。目前，宝塔服务器运维面板官方已经发布了补丁修复了漏洞，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

宝塔服务器运维面板是百塔网络科技有限公司旗下一款服务器管理软件，百塔网络科技有限公司是一个专门从事服务器相关软件及服务研发的公司。

攻击者可通过远程访问特定路径，在未授权的情况下，直接进入 phpmyadmin 数据库管理页面，以此获取服务器系统权限。

.危害影响

成功利用漏洞的攻击者可以在无需管理员授权的情况下进入数据库修改或删除数据，并且可以通过互联网远程访问管理页面，获取服务器系统权限，最终控制目标服务器。宝塔面板 Linux 版 7.4.2 版、宝塔面板 Linux 版 7.5.14 测试版、宝塔面板 Windows 版 6.8 版均受此漏洞影响。

.修复建议

目前，宝塔服务器运维面板官方已经发布了补丁修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。安全更新公告如下：

https://www.bt.cn/bbs/thread-54666-1-1.html

3.2 Apache Struts2 S2-059 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Apache Struts2 S2-059 安全漏洞（CNNVD-202008-743、CVE-2019-0230）情况的报送。成功利用漏洞的攻击者可能对目标系统执行恶意代码。Apache Struts 2.0.0–Apache Struts 2.5.20 等版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。

.漏洞介绍

Apache Struts2 是美国阿帕奇（Apache）软件基金会下属的 Jakarta 项目中的一个子项目，是一个基于 MVC 设计的 Web 应用框架。

2020 年 8 月 13 日，Apache 官方发布安全公告，修复了一个远程代码执行漏洞，编号为 S2-059 （CNNVD-202008-743、CVE-2019-0230）。该漏洞源于 Apache Struts 的框架在被强制使用时，会对标签的属性进行二次求值，最终导致远程代码执行。只有在 Struts 标签属性中强制使用 OGNL 表达式时，才能触发漏洞。

.危害影响

成功利用该漏洞的攻击者，可以在目标系统中执行恶意代码。Apache Struts 2.0.0–Apache Struts 2.5.20 等版本均受此漏洞影响。

.修复建议

目前，Apache 官方已经发布了版本更新修复了该漏洞。建议用户及时确认 Apache Struts 产品版本，如受影响，请及时采取修补措施。漏洞修补措施如下：

更新到 Struts 2.5.22 以上版本

http://struts.apache.org/download.cgi