国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 08 月 03 日-2020 年 08 月 09 日　　2020 年第 32 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 395 个，其中高危漏洞 120 个、中危漏洞 214 个、低危漏洞 61 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 47%），其中互联网上出现“wolfSSL 缓冲区过读漏洞、Encode OSS Uvicorn 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4221 个，与上周（2739 个）环比增加 54%。

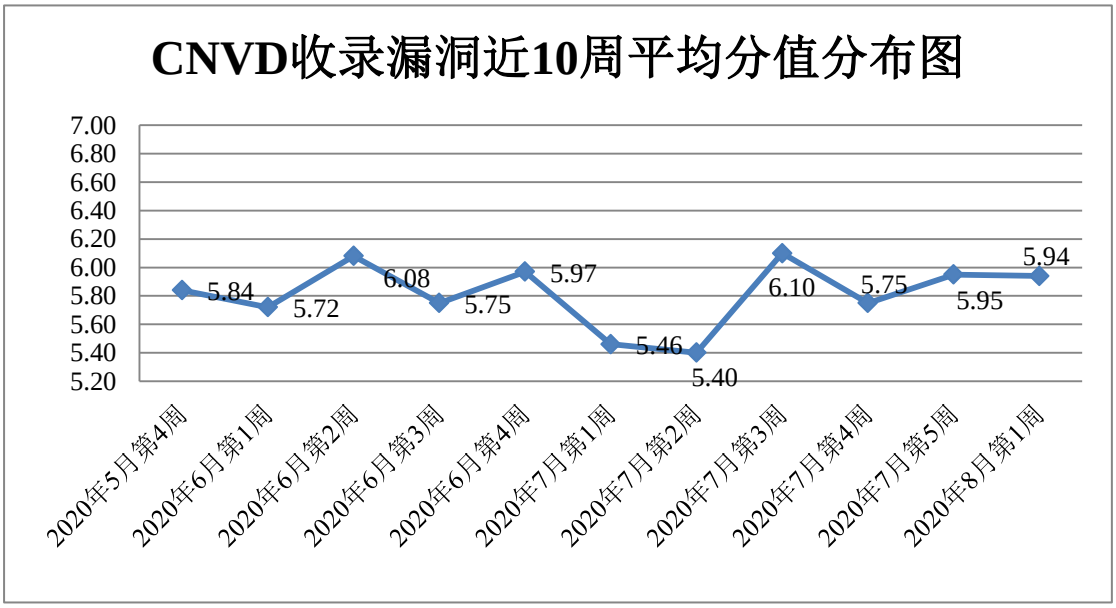

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 19 起，向基础电信企业通报漏洞事件 2 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞

事件 282 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 42 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 28 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

抚顺市众联网络技术有限公司、长沙米拓信息技术有限公司、佛山电器照明股份有限公司、哈尔滨伟成科技有限公司、杭州橙诺科技有限公司、厦门科拓通讯技术股份有限公司、杭州雄伟科技开发股份有限公司、天津市集翔企商科技有限公司、福建福昕软件开发股份有限公司、湖南火烧云信息科技有限责任公司、广西桂天能源集团有限公司、深圳市吉祥腾达科技有限公司、山西牛酷信息科技有限公司、商派软件有限公司、汉中启元动力网络有限公司、北京通达信科科技有限公司、成都汇高软件有限公司、北京辰信领创信息技术有限公司、上海商创网络科技有限公司、通用电气（GE）公司、南充优创营销策划有限公司、山东百灵健康咨询有限公司、深圳品誉实业有限公司、重庆扬浪科技有限责任公司、深圳市鼎游信息技术有限公司、上海易正信息技术有限公司、洛阳云业信息科技有限公司、西安嘉客信息科技有限责任公司、深圳市月歌科技有限公司、沈阳数业信息技术有限公司、广西雄基伟业广告有限公司、联信摩贝软件（北京）有限公司、青岛和晟思壮测控技术有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、西门子（中国）有限公司、上海纵之格科技有限公司、海南易而优科技有限公司、三鼎燃气集团有限公司、厦门三速信网络科技有限公司、廊坊市极致网络科技有限公司、金华就约我吧网络科技有限公司、海南赞赞网络科技有限公司、浙江浙大中控信息技术有限公司、东莞市鼎点网络科技有限公司、淄博闪灵网络科技有限公司、深圳警翼智能科技股份有限公司、上海卓卓网络科技有限公司、安徽希望网络科技有限公司、内蒙古万户信息科技有限公司、北京快思创杰科技有限公司安徽分公司、成都康菲顿特网络科技有限公司、快思聪电子公司、湖北淘码千维信息科技有限公司、润申信息科技（上海）有限公司、合肥明信软件技术有限公司、北京为因软件、临清市阿易网络科技、国家军民融合公共服务平台运行管理办公室、睿谷信息管理系统、Guojiz 国际网址导航系统、逍遥 B2C 商城系统、乐尚商城开源系统、逍遥 B2C 商城、贴心猫、网新科技、若依、苹果 cms、KiteCMS、CLTPHP、ZZCMS、Verydows 和 Bludit。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、华为技术有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、北京云科安信科技有限公司、山东华鲁科技发展股份有限公司、杭州迪普科技股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、河南灵创电子科技有限公司、山东道普测评技术有限公司、

内蒙古奥创科技有限公司、山东云天安全技术有限公司、吉林谛听信息技术有限公司、北京禹宏信安科技有限公司、安徽长泰信息安全服务有限公司、河南信安世纪科技有限公司、北京天地和兴科技有限公司、长春嘉诚信息技术股份有限公司、杭州安信检测技术有限公司、京东云安全、北京华云安信息技术有限公司、北京顶象技术有限公司、河北千诚电子科技有限公司、广州三零卫士信息安全有限公司、四川哨兵信息科技有限公司、郑州云智信安安全技术有限公司、上海观安信息技术股份有限公司、北京智游网安科技有限公司及其他个人白帽子向 CNVD 提交了 4221 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 3271 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
奇安信网神（补天平台）	1574	1574
斗象科技（漏洞盒子）	1162	1162
上海交大	535	535
北京神州绿盟科技有限公司	377	0
北京天融信网络安全技术有限公司	98	15
深信服科技股份有限公司	96	0
华为技术有限公司	71	0
新华三技术有限公司	58	0
北京奇虎科技有限公司	32	32
哈尔滨安天科技集团股份有限公司	22	0
北京启明星辰信息安全技术有限公司	18	1
北京知道创宇信息技术股份有限公司	8	0
国瑞数码零点实验室	140	140
北京云科安信科技有限公司	110	110
山东华鲁科技发展股份有限公司	56	56

杭州迪普科技股份有限公司	55	0
远江盛邦（北京）网络安全科技股份有限公司	50	50
河南灵创电子科技有限公司	27	27
山东道普测评技术有限公司	23	23
内蒙古奥创科技有限公司	20	20
山东云天安全技术有限公司	15	15
吉林谛听信息技术有限公司	13	13
北京禹宏信安科技有限公司	10	10
安徽长泰信息安全服务有限公司	9	9
河南信安世纪科技有限公司	7	7
北京天地和兴科技有限公司	6	6
长春嘉诚信息技术股份有限公司	5	5
杭州安信检测技术有限公司	4	4
京东云安全	4	4
北京华云安信息技术有限公司	3	3
北京顶象技术有限公司	3	3
河北千诚电子科技有限公司	3	3
广州三零卫士信息安全有限公司	1	1
四川哨兵信息科技有限公司	1	1
郑州云智信安安全技术有限公司	1	1
上海观安信息技术股份有限公司	1	1
北京智游网安科技有限公司	1	1

CNCERT 青海分中心	1	1
CNCERT 山东分中心	1	1
CNCERT 山西分中心	1	1
CNCERT 西藏分中心	3	3
CNCERT 四川分中心	1	1
个人	382	382
报送总计	5008	4221

本周漏洞按类型和厂商统计

本周，CNVD 收录了 395 个漏洞。应用程序 247 个，WEB 应用 95 个，操作系统 26 个，网络设备（交换机、路由器等网络端设备）16 个，数据库 10 个，安全产品 1 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序	247
WEB 应用	95
操作系统	26
网络设备（交换机、路由器等网络端设备）	16
数据库	10
安全产品	1

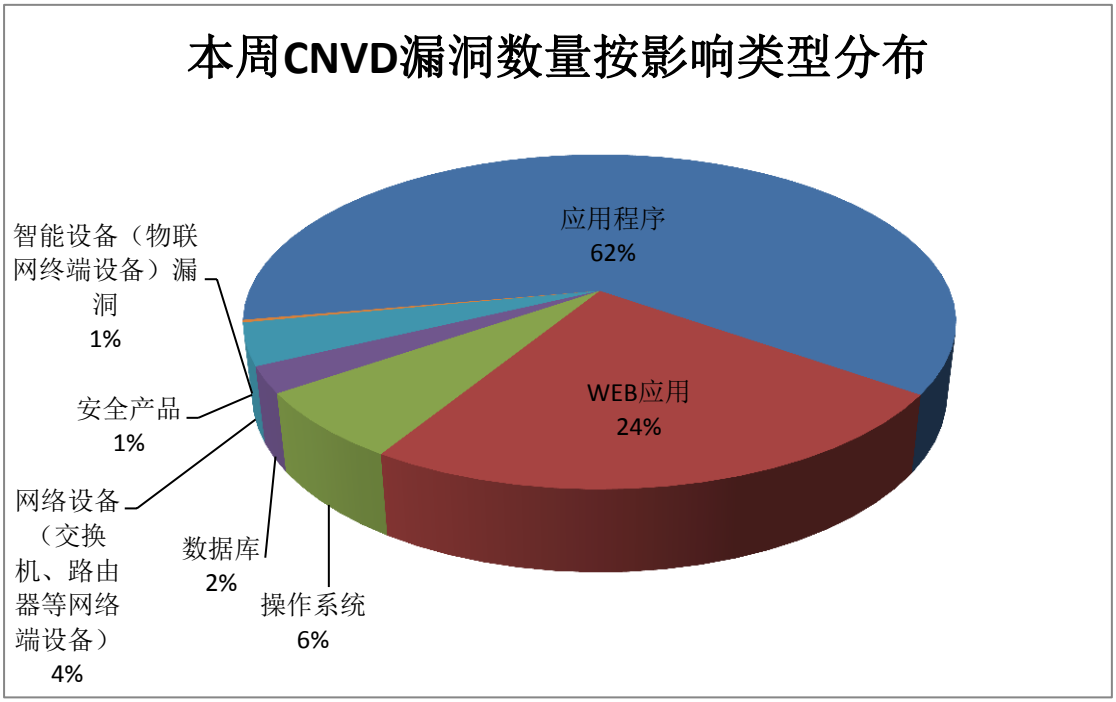

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、CentOS Web Panel、Google 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	30	8%
2	CentOS Web Panel	22	6%
3	Google	22	6%
4	IBM	21	5%
5	Cisco	18	4%
6	Adobe	12	3%
7	Mozilla	9	2%
8	Apache	8	2%
9	Grandstream	8	2%
10	其他	245	62%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，30 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Cisco Data Center Network Manager 命令注入漏洞、Teltonika TRB245 不当输入验证漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

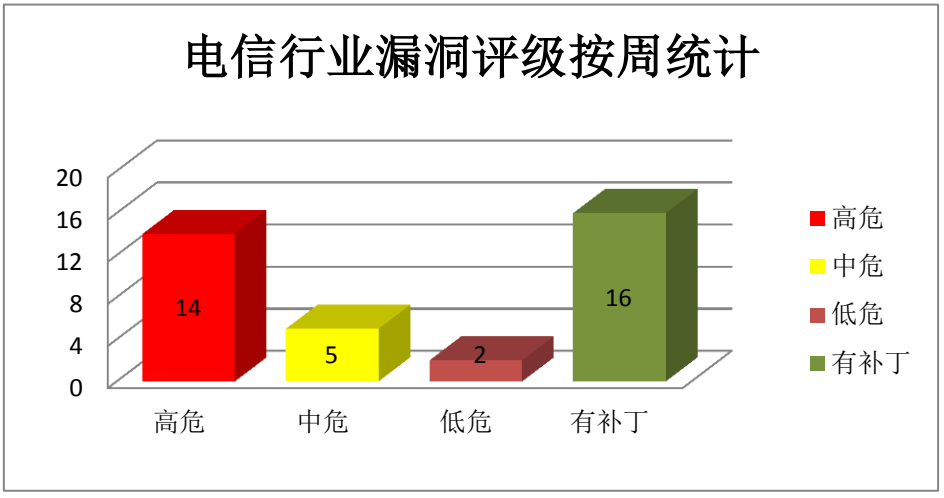

图 3 电信行业漏洞统计

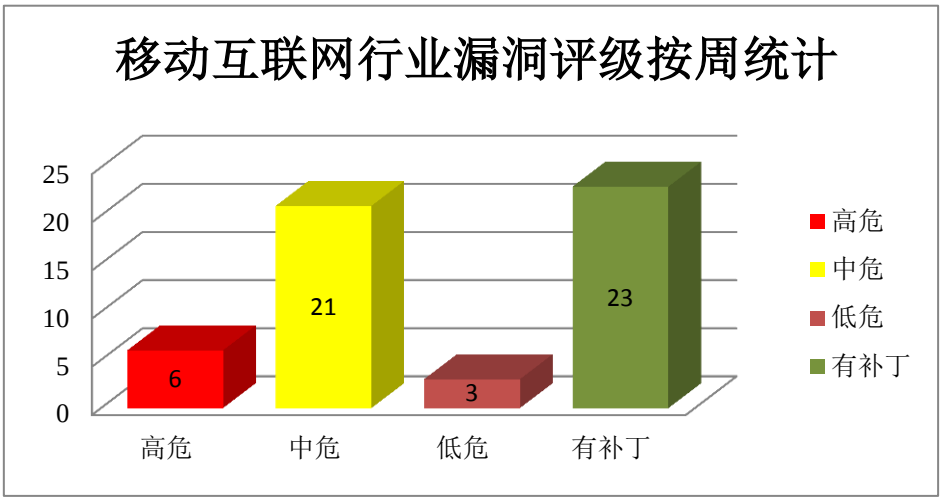

图 4 移动互联网行业漏洞统计

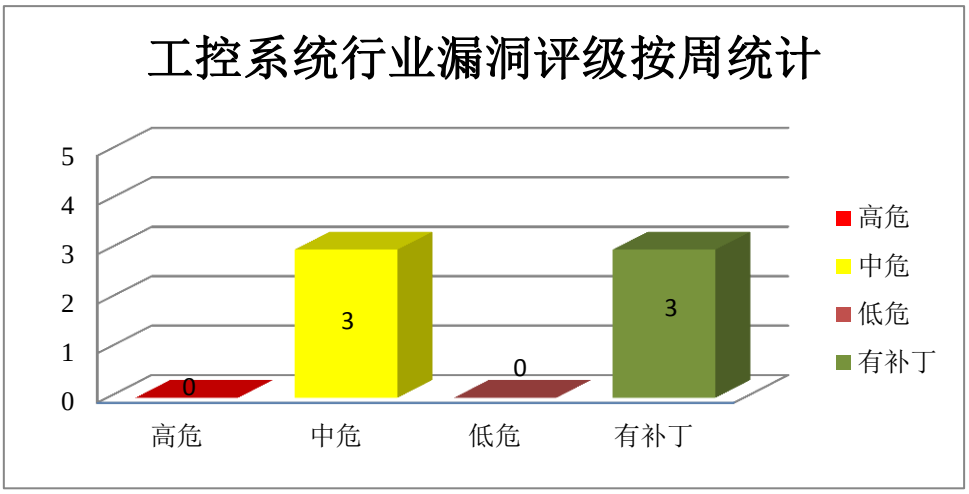

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Adobe 产品安全漏洞

Adobe Magento 是美国 Adobe 公司的一套开源的 PHP 电子商务系统。Adobe Download Manager 是一款用于管理和下载 Adobe 产品的应用程序。Adobe Media Encoder 是一款音、视频编码应用程序。Adobe Creative Cloud Desktop Application 是一套用于在 Creative 云会员管理中心管理应用程序和服务的应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞写入任意文件系统，提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Magento Commerce 和 Magento Open Source 跨站脚本漏洞、Adobe Magento Commerce 和 Magento Open Source 路径遍历漏洞、Ad

obe Download Manager 注入漏洞、Adobe Media Encoder 越界写入漏洞（CNVD-2020-44850、CNVD-2020-44851）、Adobe Creative Cloud Desktop Application 后置链接漏洞（CNVD-C-2020-154995、CNVD-2020-44854）、Adobe Creative Cloud Desktop Application 不安全文件权限漏洞。其中，除 “Adobe Media Encoder 越界写入漏洞（CNVD-2020-44850、CNVD-2020-44851）” 外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-44615
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44622
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44847
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44850
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44851
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44854
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44853
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44855

2、IBM 产品安全漏洞

IBM Verify Gateway（IVG）是美国 IBM 公司的一套基于云的身份验证解决方案。IBM WebSphere Application Server（WAS）是一款应用服务器产品。IBM Cognos Analytics 是一套商业智能软件。IBM UrbanCode Deploy（UCD）是一套应用自动化部署工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Verify Gateway (IVG)帐户锁定设置不当漏洞、IBM Verify Gateway (IVG)拒绝服务漏洞、IBM Verify Gateway (IVG)敏感信息明文传输泄露漏洞、IBM Verify Gateway (IVG)硬编码凭据漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2020-44626）、IBM Cognos Analytics 权限提升漏洞、IBM UrbanCode Deploy 代码问题漏洞、IBM Cognos Analytics XML 外部实体注入漏洞。其中，“IBM Verify Gateway (IVG)硬编码凭据漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2020-44626）、IBM UrbanCode Deploy 代码问题漏洞”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-44079
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44078
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44077
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44076
https://www.cnvd.org.cn/flaw/show/CNVD-2020-44626

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44892

https://www.cnvd.org.cn/flaw/show/CNVD-2020-45104

https://www.cnvd.org.cn/flaw/show/CNVD-2020-45109

3、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android MediaTek 组件权限提升漏洞（CNVD-2020-44361、CNVD-2020-44360、CNVD-2020-44359）、Google Android System 权限提升漏洞（CNVD-2020-44366、CNVD-2020-44367）、Google Android Media Framework 权限提升漏洞（CNVD-2020-44368）、Google Android Framework 权限提升漏洞（CNVD-2020-44375、CNVD-2020-44376）。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-44361

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44360

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44359

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44366

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44368

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44367

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44375

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44376

4、Cisco 产品安全漏洞

Cisco Data Center Network Manager（DCNM）是美国思科（Cisco）公司的一套数据中心管理系统。Cisco SD-WAN vManage Software 是一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Cisco Data Center Network Manager 信任管理问题漏洞、Cisco SD-WAN vManage Software 授权问题漏洞（CNVD-2020-44061）、Cisco Data Center Network Manager 授权问题漏洞、Cisco Data Center Network Manager 输入验证错误漏洞、Cisco Data Center Network Manager 命令注入漏洞、Cisco Data Center Network Manager 操作系统命令注入漏洞、Cisco Data Center Network Manager SQL 注入漏洞、Cisco Data Center Network Manager 访问控制错误漏洞（CNVD-2020-44067）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-44062

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44061

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44066

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44065

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44064

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44063

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44069

https://www.cnvd.org.cn/flaw/show/CNVD-2020-44067

5、Red Hat CloudForms 操作系统命令注入漏洞

Red Hat CloudForms 是美国红帽（Red Hat）公司的一套混合基础架构管理平台。本周，Red Hat CloudForms 被披露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，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-44411

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2020-42654	Citrix Systems Workspace App 访问控制错误漏洞（CNVD-2020-42654）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.citrix.com/article/CTX277662
CNVD-2020-43757	Kubevirt 权限提升漏洞	高	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://kubevirt.io/
CNVD-2020-43766	Mozilla Firefox 资源管理错误漏洞（CNVD-2020-43766）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.mozilla.org/en-US/security/advisories/mfsa2020-24/
CNVD-2020-44094	Apache Airflow 远程代码执行漏洞（CNVD-2020-44094）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread.html/r7255cf0be3566f23a768e2a04b40fb09e52fcd1872695428ba9afe91%40%3Cusers.airflow.apache.org%3E
CNVD-2020-44297	FUDForum 跨站脚本漏洞（CNVD-2020-44297）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/fudforum/code/

			6321/
CNVD-2020-44346	Grandstream HT800 series 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.grandstream.com/
CNVD-2020-44412	Red Hat CloudForms 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=1855739
CNVD-2020-44610	Pi-Hole 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://pi-hole.net/
CNVD-2020-44614	Lua 堆缓冲区溢出漏洞	高	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/lua/lua/commit/127e7a6c8942b362aa3c6627f44d660a4fb75312
CNVD-2020-44867	libMirage 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/cdemu/code/ci/0e9292c9aa34bf545f43f7efe5f0b94faba94962/
CNVD-2020-44906	Tobesoft MiPlatform 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.nexacro.com/

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞写入任意文件系统，提升权限，执行任意代码等。此外，IBM、Google、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取信息，提升权限，执行任意代码，导致拒绝服务等。另外，Red Hat CloudForms 被披露存在操作系统命令注入漏洞。攻击者可利用该漏洞执行非法操作系统命令。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、wolfSSL 缓冲区过读漏洞

验证描述

wolfSSL 是一个旨在供嵌入式系统开发人员使用的小型、可移植、嵌入式 SSL/TLS 库。

wolfSSL 4.1.0 中的 wolfcrypt/src/asn.c 中的 DecodeCertExtensions 存在缓冲区过读漏洞，该漏洞源于 GetLength_ex 的 ASN_BOOLEAN 字节读取处理错误，攻击者可通过特

制 DER 证书利用该漏洞导致缓冲区溢出。

验证信息

POC 链接：https://github.com/wolfSSL/wolfssl/issues/2421

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-44866

信息提供者

华为技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Kr00k 攻击变种影响高通和联发科 Wi-Fi 芯片

ESET 研究人员发现高通和联发科的 Wi-Fi 芯片受到 Kr00k 信息泄露漏洞的新变体的影响。新漏洞编号为 CVE-2020-3702 ，通过解除关联触发，并传输未加密的数据代替加密的数据帧，导致数据泄露，这与 Kr00k 极为相似。

参考链接：https://www.bleepingcomputer.com/news/security/kr-k-attack-variants-impact-qualcomm-mediatek-wi-fi-chips/

2. TeamViewer 曝漏洞，计算机浏览特定网页即可被无密码入侵

TeamViewer 官方发布消息说最近修复了一个漏洞，该漏洞可能使攻击者悄悄地建立与您计算机的连接并进一步利用该系统。漏洞编号为 CVE-2020-13699，该漏洞影响 TeamViewer 版本为 8,9,10,11,12,13,14,15。

参考链接：https://www.cnbeta.com/articles/tech/1013319.htm

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn
邮箱：vreport@cert.org.cn
电话：010-82991537