国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 12 月 30 日-2020 年 01 月 05 日 **2020 年第 1 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 215 个，其中高危漏洞 85 个、中危漏洞 119 个、低危漏洞 11 个。漏洞平均分值为 6.34。本周收录的漏洞中，涉及 0day 漏洞 108 个（占 50%），其中互联网上出现“Wordpress Ultimate Addons for Beaver Builder 身份验证绕过漏洞、GPAC 缓冲区溢出漏洞（CNVD-2020-00232）”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 8982 个，与上周（3493 个）环比增长 1.6 倍。

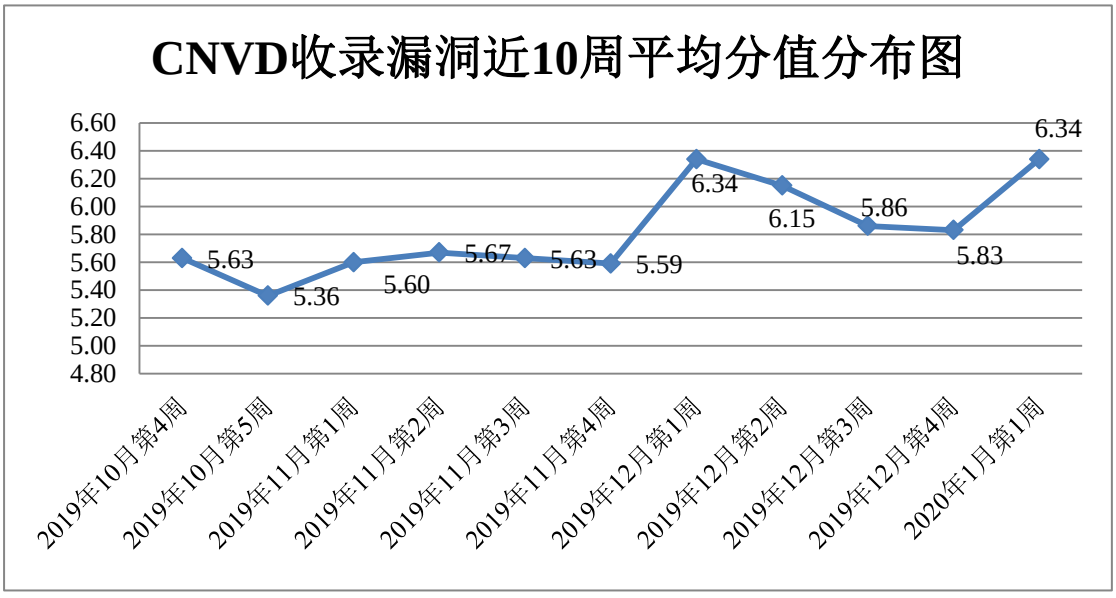

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 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 343 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 73 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 13 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：

东方财富信息股份有限公司、央视国际网络有限公司、贵州鸿宇叁柒柒科技有限公司、国药控股股份有限公司、石家庄九帆网络技术有限公司、深圳市天地心网络技术有限公司、深圳市锟锆科技有限公司、嘉兴想天信息科技有限公司深圳市常青藤软件科技有限公司、广东一一五科技股份有限公司、北京蚂蚁浏览器公司、青岛软媒网络科技有限公司、海南易而优科技有限公司、杭州简言信息科技有限公司、上海互盾信息科技有限公司、上海安达通信息安全技术股份有限公司、上海兢鑫技术开发有限公司、北京良精志诚科技有限责任公司、广州市国万电子科技有限公司、天津速读科技有限公司、茉柏枘（上海）软件科技有限公司、成都思必得信息技术有限公司、北京亚控科技发展有限公司、上海银狐信息科技有限公司、友讯电子设备（上海）有限公司、六安开发区鹏程网络工作室、广州市总工会、携程旅行网、乘风原创程序、海洋 CMS、梦雨 cms、CatfishCMS 和 WellCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、新华三技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。内蒙古洞明科技有限公司、北京铭图天成信息技术有限公司、河南灵创电子科技有限公司、山东新潮信息技术有限公司、北京华云安信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、山东云天安全技术有限公司、四川月安客信息技术有限公司、广州三零卫士信息安全有限公司、北京圣博润高新技术股份有限公司、山石网科通信技术股份有限公司、上海端御信息科技有限公司、北京智游网安科技有限公司、山东华鲁科技发展股份有限公司及其他个人白帽子向 CNVD 提交了 8982 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 8216 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）	6548	6548
斗象科技（漏洞盒子）	970	970

上海交大	698	698
北京天融信网络安全技术有限公司	209	0
哈尔滨安天科技集团股份有限公司	158	0
华为技术有限公司	116	0
新华三技术有限公司	67	0
北京神州绿盟科技有限公司	47	1
北京启明星辰信息安全技术有限公司	41	0
深信服科技股份有限公司	36	0
厦门服云信息科技有限公司	32	0
恒安嘉新(北京)科技股份公司	22	0
北京数字观星科技有限公司	19	0
四川无声信息技术有限公司	9	9
北京知道创宇信息技术股份有限公司	3	0
南京铱迅信息技术股份有限公司	2	2
内蒙古洞明科技有限公司	106	106
北京铭图天成信息技术有限公司	70	70
河南灵创电子科技有限公司	69	69
山东新潮信息技术有限公司	60	60
北京华云安信息技术有限公司	44	44
远江盛邦（北京）网络安全科技股份有限公司	39	39
国瑞数码零点实验室	15	15
杭州迪普科技股份有限公司	14	0

内蒙古奥创科技有限公司	9	9
山东云天安全技术有限公司	9	9
四川月安客信息技术有限公司	7	7
广州三零卫士信息安全有限公司	6	6
北京圣博润高新技术股份有限公司	4	4
山石网科通信技术股份有限公司	4	4
上海端御信息科技有限公司	3	3
北京智游网安科技有限公司	1	1
山东华鲁科技发展股份有限公司	1	1
CNCERT 青海分中心	16	16
CNCERT 上海分中心	16	16
CNCERT 海南分中心	9	9
CNCERT 河北分中心	4	4
CNCERT 吉林分中心	3	3
CNCERT 浙江分中心	2	2
CNCERT 甘肃分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 四川分中心	1	1
个人	254	254
报送总计	9745	8982

本周漏洞按类型和厂商统计

本周，CNVD 收录了 215 个漏洞。应用程序 96 个，WEB 应用 53 个，操作系统 28 个，网络设备（交换机、路由器等网络端设备）21 个，安全产品 16 个，智能设备（物

联网终端设备）漏洞 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	96
WEB 应用	53
操作系统	28
网络设备（交换机、路由器等网络端设备）	21
安全产品	16
智能设备（物联网终端设备）漏洞	1

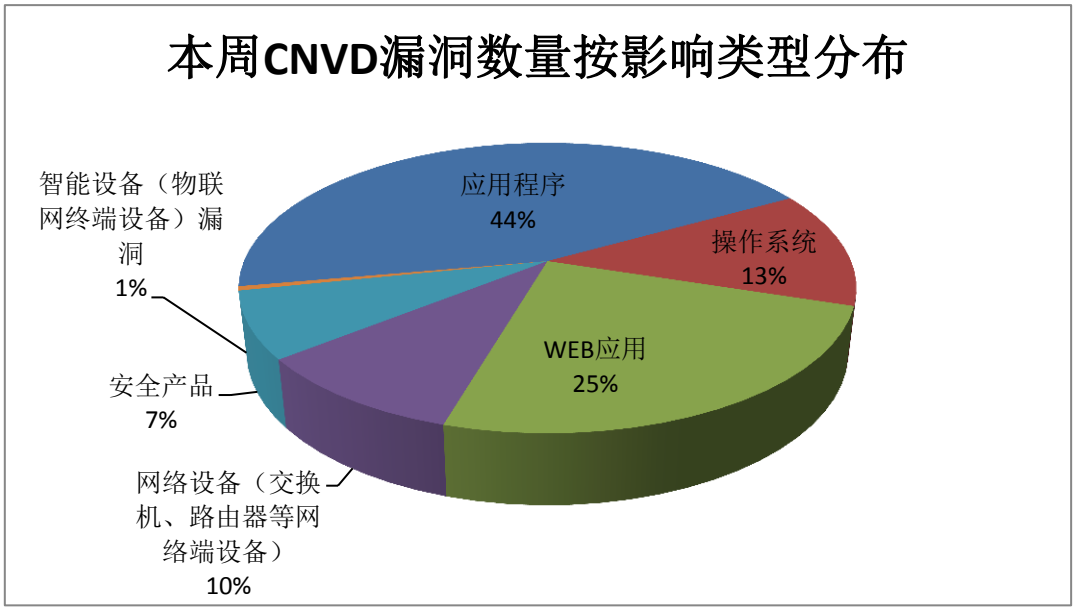

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Apple、F5 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	Cisco	20	9%
2	Apple	17	8%
3	F5	14	6%
4	Google	12	6%
5	Linux	10	5%
6	Apache	9	4%
7	Mellow Fish	6	3%
8	启明星工作室	6	3%

9	GPAC	5	2%
10	其他	116	54%

本周行业漏洞收录情况

本周，CNVD 收录了 18 个电信行业漏洞，20 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，“Tencent WeChat 命令注入漏洞、Apple iOS 和 Apple watchOS Mail Message Framework 组件资源管理错误漏洞、Cisco Data Center Network Manager SOAP API SQL 注入漏洞”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/

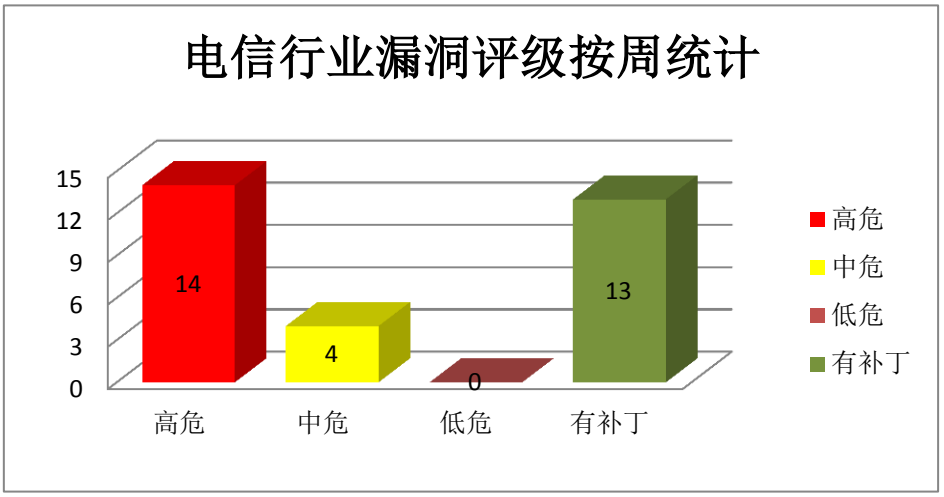

图 3 电信行业漏洞统计

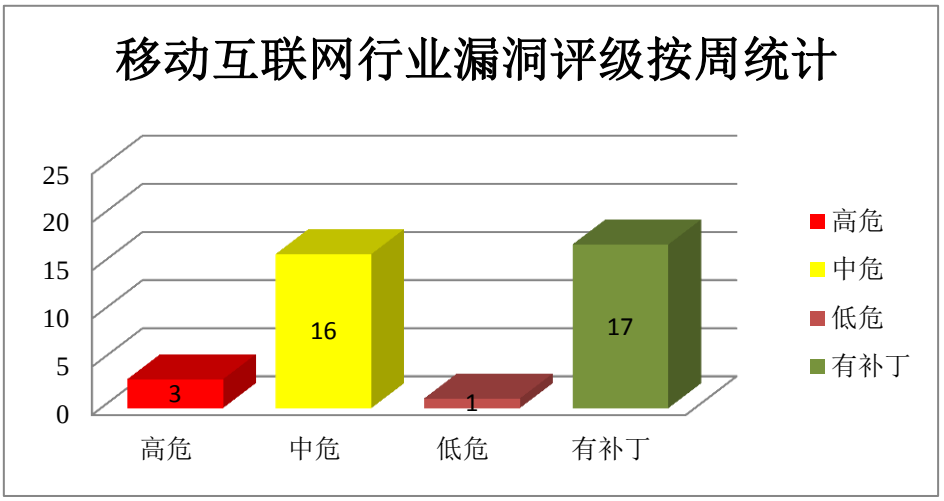

图 4 移动互联网行业漏洞统计

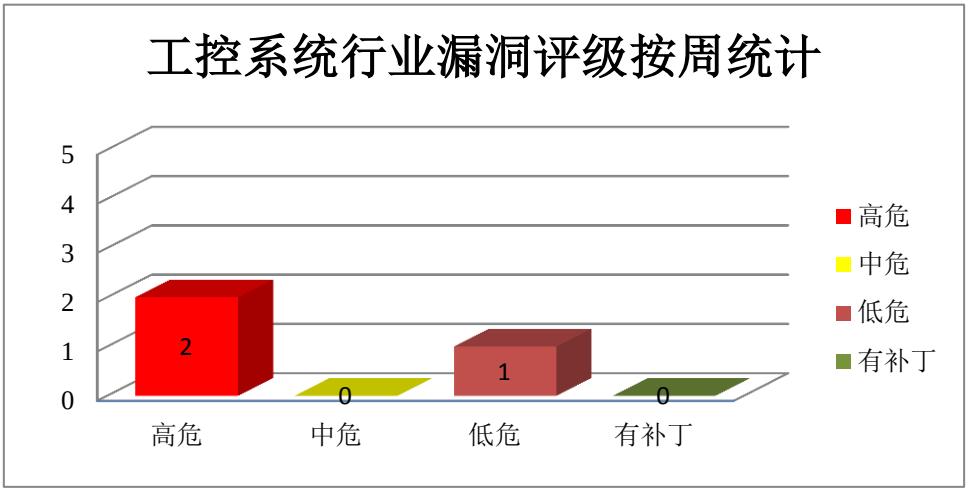

图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco Data Center Network Manager (DCNM)是一套数据中心网络管理器，可对网络进行多协议管理，并对交换机的运行状况和性能提供故障排除功能。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数据库敏感信息，执行未授权操作，注入任意命令等。

CNVD 收录的相关漏洞包括：Cisco Data Center Network Manager SOAP API 路径遍历漏洞、Cisco Data Center Network Manager REST API SQL 注入漏洞、Cisco Data Center Network Manager SOAP API SQL 注入漏洞、Cisco Data Center Network Manager REST API 认证绕过漏洞、Cisco Data Center Network Manager SOAP API 认证绕过漏洞、Cisco Data Center Network Manager REST API 命令注入漏洞、Cisco Data Center Network Manager SOAP API 命令注入漏洞、Cisco Data Center Network Manager REST API 路径遍历漏洞。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-00280

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00281

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00282

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00283

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00284

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00288

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00289

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00290

2、F5 产品安全漏洞

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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成内存泄露，导致拒绝服务（系统资源耗尽），提升权限，修改配置并执行任意的系统命令。

CNVD 收录的相关漏洞包括：F5 BIG-IP 输入验证错误漏洞（CNVD-2020-00236、CNVD-2020-00238、CNVD-2020-00237、CNVD-2020-00244、CNVD-2020-00242）、F5 BIG-IP 资源管理错误漏洞（CNVD-2020-00240）、F5 BIG-IP 权限提升漏洞、F5 BIG-IP tmrouted 内存泄露漏洞。其中，“F5 BIG-IP 输入验证错误漏洞（CNVD-2020-00236）、F5 BIG-IP tmrouted 内存泄露漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-00236

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00238

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00237

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00240

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00244

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00245

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00242

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00243

3、Apple 产品安全漏洞

Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。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受影响组件敏感信息，执行远程代码，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 组件缓冲区溢出漏洞（CNVD-2020-00207、CNVD-2020-00204、CNVD-2020-00209、CNVD-2020-00210、CNVD-2020-00213）、Apple iOS、tvOS 和 watchOS Wi-Fi 组件信息泄露漏洞、Apple iOS 和 Apple watchOS Mail 组件输入验证错误漏洞、Apple iOS 和 Apple watchOS Mail Message Framework 组件资源管理错误漏洞。其中，“Apple iOS 和 Apple watchOS Mail Message Framework 组件资源管理错误漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-00207

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00204
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00208
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00209
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00210
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00211
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00212
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00213

4、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞伪造 Omnibox 内容，执行任意代码，造成堆损坏。

CNVD 收录的相关漏洞包括：Google Chrome WebSockets 资源管理错误漏洞、Google Chrome JavaScript 缓冲区溢出漏洞、Google Chrome 缓冲区溢出漏洞（CNVD-2020-00271）、Google Chrome JavaScript 组件缓冲区溢出漏洞（CNVD-2020-00275、CNVD-2020-00479、CNVD-2020-00480）、Google TensorFlow 缓冲区溢出漏洞、Google Chrome 输入验证错误漏洞（CNVD-2020-00482）。其中，“Google TensorFlow 缓冲区溢出漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-00273
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00272
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00271
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00275
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00479
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00480
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00481
http://www.cnvd.org.cn/flaw/show/CNVD-2020-00482

5、SonicWall SMA100 缓冲区溢出漏洞

SonicWall SMA100 是一款安全访问网关设备。本周，SonicWall SMA100 被披露存在缓冲区溢出漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-00278

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-2020-00215	Huawei USG9500 拒绝服务漏洞（CNVD-2020-00215）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20191225-01-eudemon-cn
CNVD-2020-00241	Tencent WeChat 命令注入漏洞	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：http://www.tencent.com/
CNVD-2020-00276	ImageMagick Studio ImageMagick 缓冲区溢出漏洞（CNVD-2020-00276）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ImageMagick/ImageMagick/issues/1562
CNVD-2020-00481	Google TensorFlow 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://github.com/tensorflow/tensorflow/commit/db4f9717c41bccc3ce10099ab61996b246099892
CNVD-2020-00490	Microsoft Windows Windows Printer Service 提权漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-1477
CNVD-2020-00491	ShapeShift KeepKey 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://github.com/keepkey/keepkey-firmware/commit/b222c66cdd7c3203d917c80ba615082d309d80c3
CNVD-2020-00503	Apache Tomcat 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://tomcat.apache.org/security-9.html
CNVD-2020-00507	OmniOS Community Edition illumos 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://omniosce.org/
CNVD-2020-00216	Huawei USG9500 拒绝服务漏洞（CNVD-2020-00216）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20191225-01-eudemon-cn
CNVD-2020-00501	Apache Atlas 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/cc21437c4c5053a13e13332d614d5172f39da

			03491fe17ae260be221@%3Cdev.atlas.apache.org%3E

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息，执行未授权操作，注入任意命令等。此外，F5、Apple、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，执行远程代码，导致缓冲区溢出或堆溢出等。另外，SonicWall SMA100 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。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、Wordpress Ultimate Addons for Beaver Builder 身份验证绕过漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

Wordpress Ultimate Addons for Beaver Builder 存在认证绕过漏洞，该漏洞源于网络系统或产品中缺少身份验证措施或身份验证强度不足，攻击者可利用漏洞绕过某些安全限制并执行未经授权的操作。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2020010002

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-00505

信息提供者

深信服科技股份有限公司

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. 儿童智能手表爆高危漏洞，黑客能轻易追踪孩子

近期，有多家国外媒体曝出国内儿童智能手表供应商存在安全防护漏洞问题，黑客发现这些安全漏洞不仅能检索或改变儿童的实时 GPS 位置，还可以给他们打电话，或者悄悄监视孩子的活动范围。据估计，至少有 4700 万的终端设备可能受此影响。有用户调侃，对于这些劣质的儿童智能手表，定位不精准或许成了它们最大的优点。

参考链接：http://tech.163.com/19/1231/10/F1NG7EMM000999LD.html

2. 物联网供应商 Wyze 确认服务器数据泄漏

Wyze 是一家销售安全设备的物联网公司，如安全摄像机、智能插头、智能灯泡和智能门锁等。该公司昨日证实发生了服务器数据泄漏事件，该事件泄露了大约 240 万客户的详细信息。此外，该 240 万用户的详细信息在网上暴露了 22 天。

参考链接：https://www.freebuf.com/news/224108.html

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