国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 05 月 04 日-2020 年 05 月 10 日　　2020 年第 19 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 715 个，其中高危漏洞 331 个、中危漏洞 316 个、低危漏洞 68 个。漏洞平均分值为 6.39。本周收录的漏洞中，涉及 0day 漏洞 512 个（占 72%），其中互联网上出现“PHP-Fusion 'Edit Profile'任意文件上传漏洞、Internet Download Manager 堆栈缓冲区溢出漏洞”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 5514 个，与上周（3232 个）环比增加 71%。

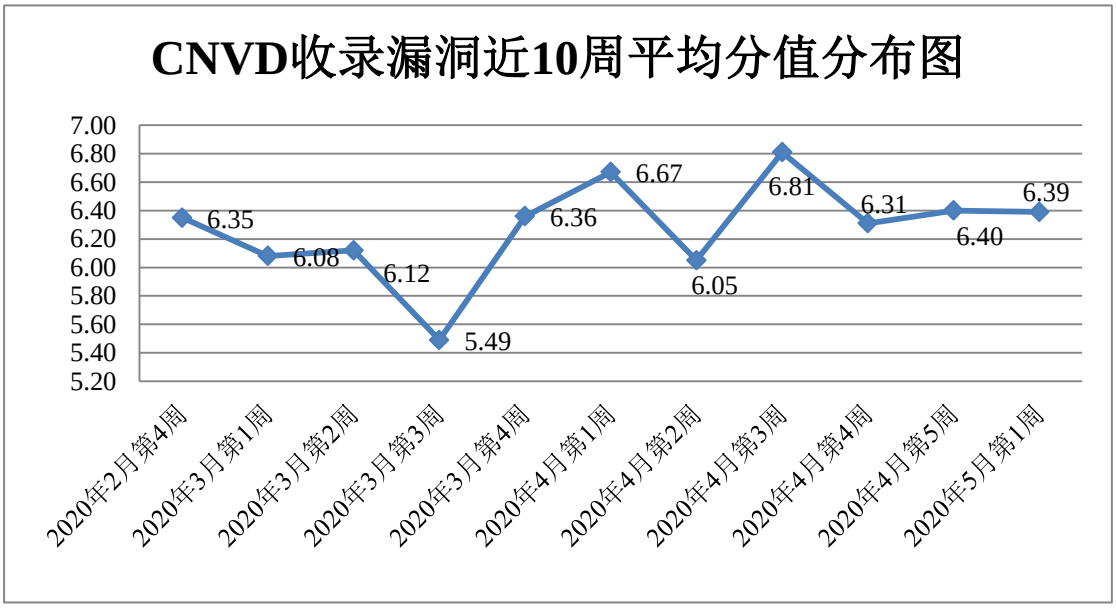

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 38 起，向基础电信企业通报漏洞事件 8 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 216 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 20 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 25 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：

上海丹帆网络科技有限公司、网件（北京）网络技术有限公司、成都爱诚科技有限公司、长沙友点软件科技有限公司、陕西新势力网络科技有限公司、海南赞赞网络科技有限公司、哈尔滨伟成科技有限公司、沈阳点动科技有限公司、成都我趣科技有限公司、深圳市三齐自动化科技有限公司、北京酷我科技有限公司、龙采科技集团有限责任公司、谷歌公司、宁波高新区奥凯网络科技有限公司、石家庄市征红网络科技有限公司、成都天问互联科技有限公司、苏州烟火网络科技有限公司、西安惠天网络科技有限公司、北京知变科技有限公司、武汉初心科技有限公司、淄博闪灵网络科技有限公司、昆山东云网络科技有限公司、深圳市圆梦云科技有限公司、北京通达信科科技有限公司、杭州飞致云信息科技有限公司、北京良精志诚科技有限责任公司、北京金方时代科技有限公司、北京亚控科技发展有限公司、广州星外信息科技有限公司、深圳神州通达网络技术有限公司、济南亘安信息技术有限公司、海南易而优科技有限公司、居易科技股份有限公司、西安佰联网络技术有限公司、武汉衍艺广告有限公司、深圳银澎云计算有限公司、三菱电机自动化（中国）有限公司、佛山云迈电子商务有限公司、青岛商至信网络科技有限公司、太原迅易科技有限公司、宁波高新区众宇网络有限公司、长园深瑞继保自动化有限公司、郑州索特信息技术有限公司、中交一公局集团有限公司、开平市联科网络科技有限公司、湖南翱云网络科技有限公司、上海商派网络科技有限公司、重庆光大网络技术有限公司、伟创互联网络技术开发团队、清华大学信息化技术中、易迅软件工作室、诚技博源网络科技、贴心猫(imcat)、网展科技、品优影视、百易网络、逍遥 B2C 商城系统、海洋 CMS、PopojiCMS、Catfish CMS、YCCMS、Heybbs、115CMS、ShyPost、zzzcms 和 TOTOLINK。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，恒安嘉新(北京)科技股份公司、新华三技术有限公司、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、华为技术有限公司等单位报送公开收集的漏洞数量较多。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、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、上海观安信息技术股份有限公司、北京天地和兴科技有限公司、北京华云安信息技术有限公司、河南信安世纪科技有限公司、北京圣博润高新技术股份有限公司、山东云天安全技术有限公司、北京智游网安科技有限公司、北京墨云科技有限公司、北京丁牛科技有限公司、安徽风雪网络安全测评有限公司、农

信银资金清算中心、山东新潮信息技术有限公司、郑州赛欧思科技有限公司及其他个人白帽子向 CNVD 提交了 5514 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 4952 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）	3646	3646
斗象科技（漏洞盒子）	769	769
上海交大	537	537
恒安嘉新(北京)科技股份公司	292	0
新华三技术有限公司	240	0
北京天融信网络安全技术有限公司	186	1
哈尔滨安天科技集团股份有限公司	167	0
华为技术有限公司	108	0
深信服科技股份有限公司	77	0
北京奇虎科技有限公司	77	48
北京启明星辰信息安全技术有限公司	72	2
北京数字观星科技有限公司	59	0
北京神州绿盟科技有限公司	48	6
中国电信集团系统集成有限责任公司	4	0
杭州安恒信息技术股份有限公司	3	3
北京知道创宇信息技术股份有限公司	2	0
远江盛邦（北京）网络安全科技股份有限公司	66	66
国瑞数码零点实验室	50	50

内蒙古奥创科技有限公司	36	36
北京铭图天成信息技术有限公司	26	26
河南灵创电子科技有限公司	18	18
上海观安信息技术股份有限公司	10	10
北京天地和兴科技有限公司	4	4
北京华云安信息技术有限公司	3	3
河南信安世纪科技有限公司	3	3
北京圣博润高新技术股份有限公司	2	2
山东云天安全技术有限公司	2	2
北京智游网安科技有限公司	1	1
北京墨云科技有限公司	1	1
北京丁牛科技有限公司	1	1
安徽风雪网络安全测评有限公司	1	1
农信银资金清算中心	1	1
山东新潮信息技术有限公司	1	1
郑州赛欧思科技有限公司	1	1
河北分中心	12	12
青海分中心	6	6
西藏分中心	2	2
贵州分中心	1	1
河南分中心	1	1
吉林分中心	1	1

四川分中心	1	1
个人	251	251
报送总计	6789	5514

本周漏洞按类型和厂商统计

本周，CNVD 收录了 715 个漏洞。WEB 应用 337 个，应用程序 250 个，网络设备（交换机、路由器等网络端设备）77 个，操作系统 28 个，智能设备（物联网终端设备）16 个，安全产品 6 个，数据库 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
WEB 应用	337
应用程序	250
网络设备（交换机、路由器等网络端设备）	77
操作系统	28
智能设备（物联网终端设备）	16
安全产品	6
数据库	1

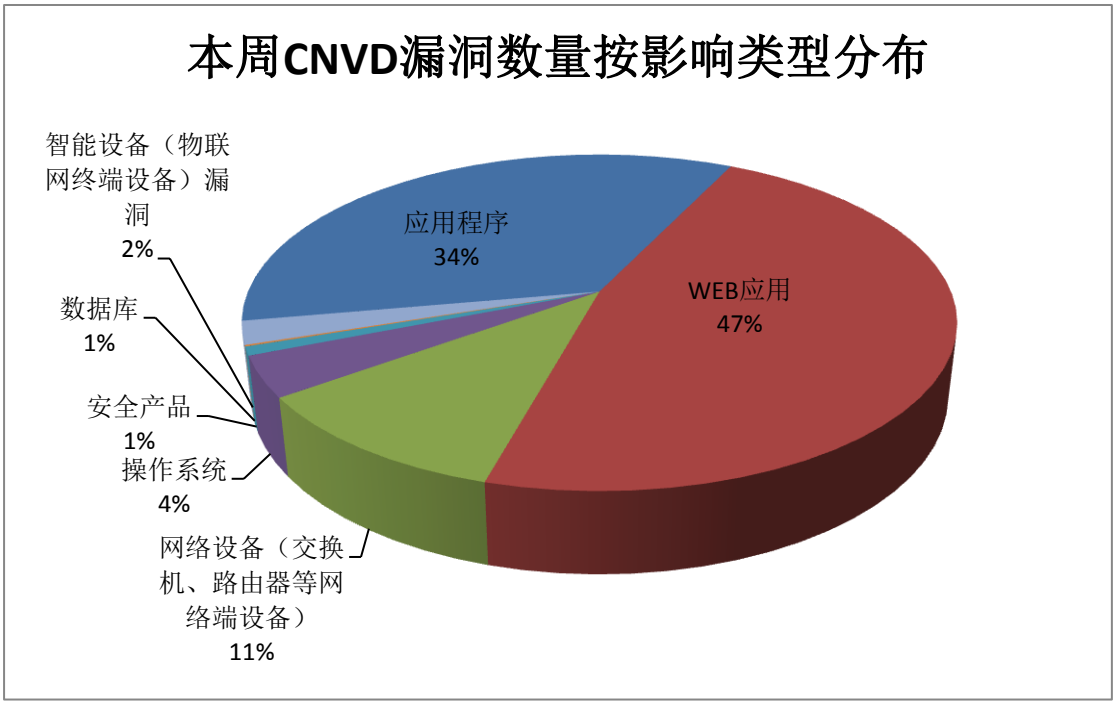

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 NETGEAR、Oracle、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	NETGEAR	60	8%
2	Oracle	27	3%
3	Google	21	3%
4	哈尔滨伟成科技有限公司	17	2%
5	深圳市腾讯计算机系统有限公司	14	2%
6	WordPress	13	2%
7	Rukovoditel	12	2%
8	Heybbs 微社区	11	2%
9	Huawei	11	2%
10	其他	529	74%

本周行业漏洞收录情况

本周，CNVD 收录了 63 个电信行业漏洞，43 个移动互联网行业漏洞，18 个工控行业漏洞（如下图所示）。其中，“Huawei AR3200 授权问题漏洞、多款 NETGEAR 产品命令注入漏洞（CNVD-2020-26954）、Xiaomi Mi WiFi R3G 命令注入漏洞、Google Android System 权限提升漏洞（CNVD-2020-27128）”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/

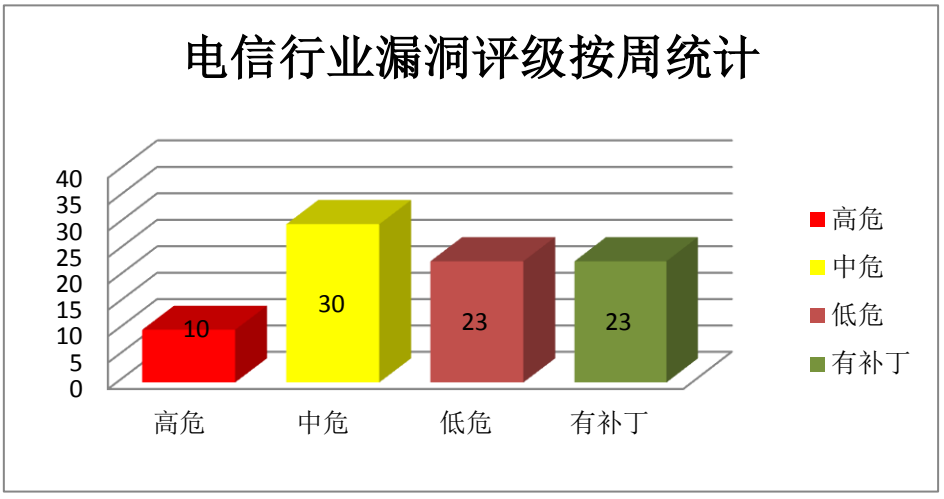

图 3 电信行业漏洞统计

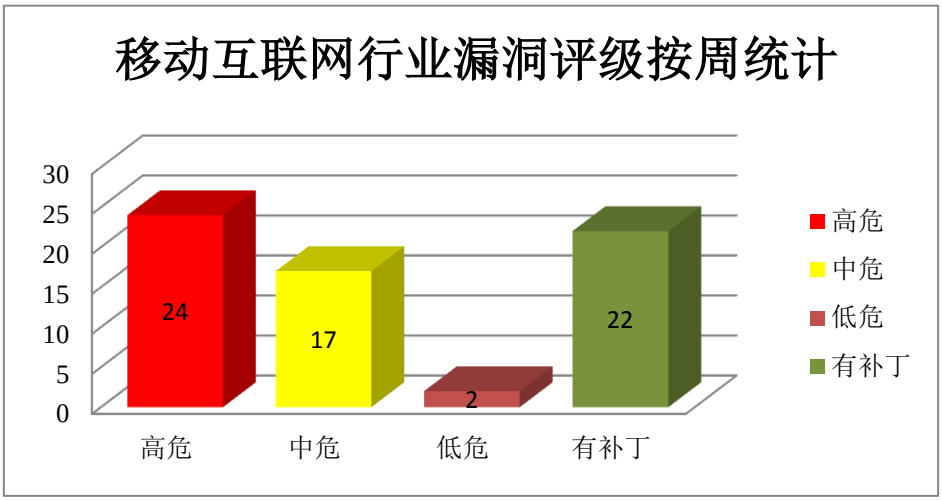

图 4 移动互联网行业漏洞统计

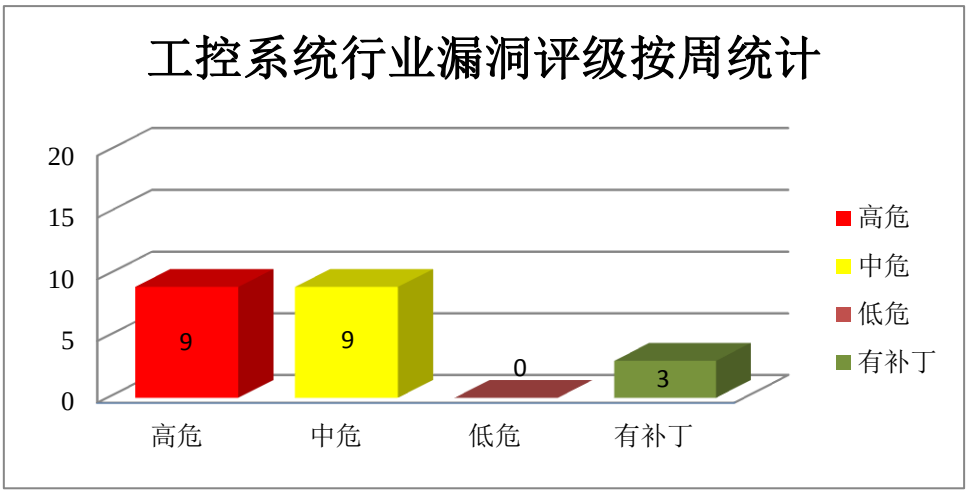

图 5 工控系统行业漏洞统计

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、 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，攻击者可利用漏洞升权限。

CNVD 收录的相关漏洞包括：Google Android System 权限提升漏洞（CNVD-2020-27126、CNVD-2020-27124、CNVD-2020-27128、CNVD-2020-27127）、Google Android Framework 权限提升漏洞（CNVD-2020-27135、CNVD-2020-27134、CNVD-2020-27136）、Google Android Media framework 权限提升漏洞（CNVD-2020-27133）。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-2020-27126
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27124
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27128
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27127
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27135
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27134
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27133
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27136

2、Huawei 产品安全漏洞

Huawei Honor V10 是一款智能手机产品。Huawei Lion-AL00C 是一款智能手机。Huawei ODS 是一款基于对象的存储设备。Huawei PCManager 是一套电脑管理软件。Huawei AR3200 是一款企业级路由器。Huawei Taurus-AL00B 是一款智能手机。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设备部分权限，造成信息泄露，导致设备异常（拒绝服务）。

CNVD 收录的相关漏洞包括：Huawei Honor V10 越界读漏洞（CNVD-2020-27112、CNVD-2020-27116、CNVD-2020-27114）、Huawei Lion-AL00C 输入验证错误漏洞、Huawei OSD 权限提升漏洞、Huawei PCManager 权限提升漏洞（CNVD-2020-27120）、Huawei AR3200 授权问题漏洞、Huawei Taurus-AL00B 信息泄露漏洞。其中，“Huawei AR3200 授权问题漏洞”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-2020-27112
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27116
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27114
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27118
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27117
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27120
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27119
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27125

3、Cisco 产品安全漏洞

Cisco Firepower Threat Defense（FTD）是一套提供下一代防火墙服务的统一软件。Cisco Hosted Collaboration Mediation Fulfillment（HCM-F）是一款托管协作解决方案（HCS）的核心管理组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感数据，将用户重定向到特定的恶意网页，以 root 用户访问权限运行任何系统命令等。

CNVD 收录的相关漏洞包括：Cisco Firepower Threat Defense 数据伪造问题漏洞、

Cisco Firepower Threat Defense 访问控制错误漏洞（CNVD-2020-27106、CNVD-2020-27107）、Cisco Firepower Management Center 输入验证错误漏洞（CNVD-2020-27105）、Cisco Firepower Management Center 信任管理问题漏洞、Cisco Firepower Management Center 输入验证错误漏洞（CNVD-2020-27103）、Cisco Firepower Management Center 跨站脚本漏洞（CNVD-2020-27108）、Cisco Hosted Collaboration Mediation Fulfillment 代码问题漏洞。其中，“Cisco Firepower Management Center 信任管理问题漏洞”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-2020-27102
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27106
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27105
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27104
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27103
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27108
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27109
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27107

4、WordPress 产品安全漏洞

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，提升权限，执行客户端代码等。

CNVD 收录的相关漏洞包括：WordPress 访问限制绕过漏洞（CNVD-2020-27079）、WordPress 跨站脚本漏洞（CNVD-2020-27078、CNVD-2020-27082、CNVD-2020-27081）、WordPress Advanced Woo Search 信息泄露漏洞、WordPress mappress-google-maps-for-wordpress 代码问题漏洞、WordPress 权限提升漏洞（CNVD-2020-27089）、WordPress data-tables-generator-by-supsystic 跨站请求伪造漏洞。其中，除“WordPress 跨站脚本漏洞（CNVD-2020-27078、CNVD-2020-27082、CNVD-2020-27081）”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-2020-27079
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27078
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27082
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27081
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27084
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27085
https://www.cnvd.org.cn/flaw/show/CNVD-2020-27089

https://www.cnvd.org.cn/flaw/show/CNVD-2020-27087

5、ABBS Software Audio Media Player 缓冲区溢出漏洞

ABBS Software Audio Media Player 是一款音频播放器。本周，ABBS Software Audio Media Player 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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-27091

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-2020-26846	BMC Control-M/Agent 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.bmc.com/it-solutions/control-m.html
CNVD-2020-26853	Autodesk FBX-SDK 类型混淆漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.autodesk.com/trust/security-advisories/adsk-sa-2020-0002
CNVD-2020-26948	多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2020-26948）	高	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/000061504/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-Some-Routers-and-Gateways-PSV-2018-0304
CNVD-2020-27104	Cisco Firepower Management Center 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcua-statcred-weeCcZct
CNVD-2020-27110	Apple macOS Catalina Printing 组件权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/en-us/HT211100
CNVD-2020-27119	Huawei AR3200 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://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20200422-01-authentication-cn

CNVD-2020-27226	HANDYSOFT Handy Groupware 操作系统命令注入漏洞	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.handysoft.co.kr/
CNVD-2020-27281	Lenovo System Interface Foundation 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.lenovo.com/us/en/product_security/LEN-30401
CNVD-2020-27432	Advantech WebAccess Node 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://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download
CNVD-2020-27444	Accellion File Transfer Appliance 操作系统命令注入漏洞	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：https://www.accellion.com/

小结：本周，Google 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。此外 Huawei、Cisco、WordPress 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，提升权限，执行客户端代码，导致设备异常（拒绝服务）等。另外，ABBS Software Audio Media Player 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、Internet Download Manager 堆栈缓冲区溢出漏洞

验证描述

Internet Download Manager 是一款下载工具，提供断点续传等多种功能。

Internet Download Manager 存在堆栈缓冲区溢出漏洞。攻击者可通过提升本地进程权限来破坏文件系统。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35388

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-27196

信息提供者

CNVD 工作组

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. 特斯拉二手车被曝隐私问题，黑客获得大量个人信息

据外媒报道，特斯拉的车载计算机系统，可能没有大家想象的那么安全。根据某一网络安全研究员的说法，即便在完全恢复出厂设置后，黑客依旧可以从旧的特斯拉面板系统中恢复大量个人信息。

参考链接：https://finance.sina.com.cn/stock/relnews/us/2020-05-07/doc-iircuyvi1767329.shtml

2. LineageOS、Ghost 和 DigiCert 服务器遭黑客入侵

近日，黑客利用了两个最近披露的 Salt 漏洞入侵了 LineageOS、Ghost 和 DigiCert 的服务器。Salt 是是一个监视和更新服务器状态的开源配置工具。上周安全公司 F-Secure 的研究人员披露了两个漏洞 CVE-2020-11651 和 CVE-2020-11652，允许远程攻击者绕过身份验证和授权控制，以 root 权限执行命令。

参考链接：https://www.solidot.org/story?sid=64269

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