国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 02 月 24 日-2020 年 03 月 01 日　　2020 年第 9 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 699 个，其中高危漏洞 288 个、中危漏洞 327 个、低危漏洞 84 个。漏洞平均分值为 6.35。本周收录的漏洞中，涉及 0day 漏洞 309 个（占 44%），其中互联网上出现“Rasilient PixelStor 5000 远程代码执行漏洞、WordPress Theme Fruitful 跨站脚本漏洞”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 2413 个，与上周（4336 个）环比减少 44%。

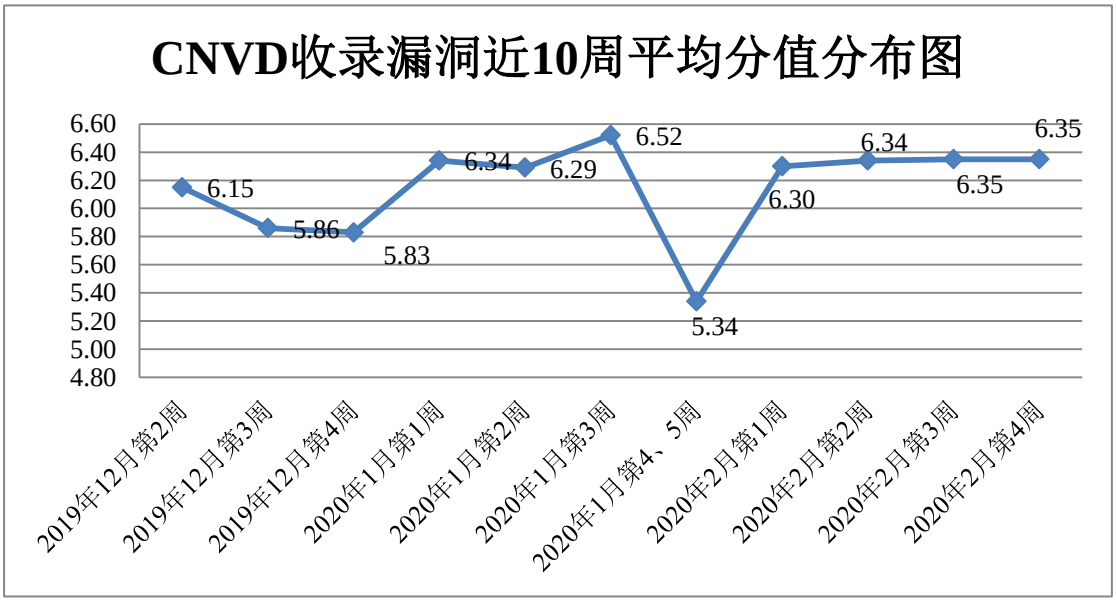

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电信企业通报漏洞事件 13 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 391 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 70 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：

南京云恩通讯科技有限公司、烟台云脉网络科技有限公司、海南赞赞网络科技有限公司、广州齐博网络科技有限公司、北京搜狗信息服务有限公司、深圳市迪元素科技有限公司、苏州乐艺网络科技有限公司、合肥一浪网络科技有限公司、成都领城信息技术有限公司、广州永拓信息科技有限公司、海南创想未来文化传媒有限公司、苏州科达科技股份有限公司、金山软件股份有限公司、北京世纪超星信息技术发展有限责任公司、北京椒图科技有限公司、台达电子企业管理(上海)有限公司、昆明云涛科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江宇视科技有限公司、青岛商至信网络科技有限公司、青岛网搜网络技术有限公司、青岛灼灼文化传媒有限公司、南通协达软件有限公司、淄博闪灵网络科技有限公司、长沙米拓信息技术有限公司、东莞市百塔网络科技有限公司、中铁八局集团第三工程有限公司、石家庄市征红网络科技有限公司、沈阳点动科技有限公司、上海格诗网络科技有限公司、苏州托普斯网络科技有限公司、搜狗公司、深圳市大点科技有限公司、杭州可道云网络有限公司、上海秀可视科技有限公司、湖北淘码千维信息科技有限公司、南充市老虎云网络技术有限公司、湖南翱云网络科技有限公司、名炬企业管理（上海）有限公司、厦门海为科技有限公司、青岛易企天创管理咨询有限公司、国药控股北京有限公司、西安瑞友信息技术资讯有限公司、北京和利时自动化驱动技术有限公司、洪湖尔创网联信息技术有限公司、佛山市搜虎网络科技有限公司、深圳市锟锆科技有限公司、长沙友点软件科技有限公司、开平市联科网络科技有限公司、深圳前海小树时代互联网金融服务有限公司、和利时集团、猎豹移动公司、新秀工作室、乐清翰珂网络、优艺 cms、SemCms、FTDMS、UQCMS、pigcloud、ZrLog 和 BEESCMS。

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、北京神州绿盟科技有限公司、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。四川无声信息技术有限公司、中国电信集团系统集成有限责任公司、远江盛邦（北京）网络安全科技股份有限公司、长春嘉诚信息技术股份有限公司、北京华云安信息技术有限公司、内蒙古洞明科技有限公司、山东新潮信息技术有限公司、南京众智维信息科技有限公司、北京铭图天成信息技术有限公司、北京圣博润高新技术股份有限公司、北京机沃科技有限公司、国瑞数码零

点实验室、北京长亭科技有限公司、内蒙古奥创科技有限公司、山石网科通信技术股份有限公司、四川哨兵信息科技有限公司、河南灵创电子科技有限公司、河南信安世纪科技有限公司、鼎信信息科技有限责任公司、山东云天安全技术有限公司、厦门靠谱云股份有限公司、北京智游网安科技有限公司、博智安全科技股份有限公司、深圳市魔方安全科技有限公司、南瑞集团公司（国网电力科学研究院）、上海观安信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 2413 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 1050 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
上海交大	407	407
斗象科技（漏洞盒子）	327	327
奇安信网神（补天平台）	316	316
北京天融信网络安全技术有限公司	270	15
四川无声信息技术有限公司	156	156
哈尔滨安天科技集团股份有限公司	153	0
华为技术有限公司	120	0
北京神州绿盟科技有限公司	114	1
新华三技术有限公司	78	0
恒安嘉新(北京)科技股份公司	73	0
深信服科技股份有限公司	72	0
中国电信集团系统集成有限责任公司	63	63
北京启明星辰信息安全技术有限公司	50	0
北京数字观星科技有限公司	38	0
西安四叶草信息技术有限公司	15	15

南京联成科技发展股份有限公司	3	3
南京铱迅信息技术股份有限公司	3	3
北京知道创宇信息技术有限公司	2	0
远江盛邦（北京）网络安全科技股份有限公司	244	244
长春嘉诚信息技术股份有限公司	92	92
北京华云安信息技术有限公司	84	84
内蒙古洞明科技有限公司	62	62
山东新潮信息技术有限公司	60	60
南京众智维信息科技有限公司	30	30
杭州迪普科技股份有限公司	26	0
北京铭图天成信息技术有限公司	26	26
北京圣博润高新技术股份有限公司	24	24
北京机沃科技有限公司	21	21
国瑞数码零点实验室	16	16
北京长亭科技有限公司	10	10
内蒙古奥创科技有限公司	8	8
山石网科通信技术股份有限公司	7	7
四川哨兵信息科技有限公司	7	7
河南灵创电子科技有限公司	5	5
河南信安世纪科技有限公司	5	5
鼎信信息科技有限责任公司	3	3
山东云天安全技术有限公司	3	3

厦门靠谱云股份有限公司	2	2
北京智游网安科技有限公司	1	1
博智安全科技股份有限公司	1	1
深圳市魔方安全科技有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
上海观安信息技术股份有限公司	1	1
CNCERT 江西分中心	8	8
CNCERT 河北分中心	7	7
CNCERT 黑龙江分中心	6	6
CNCERT 湖南分中心	6	6
CNCERT 吉林分中心	4	4
CNCERT 内蒙古分中心	4	4
CNCERT 上海分中心	3	3
CNCERT 甘肃分中心	2	2
CNCERT 海南分中心	2	2
CNCERT 广西分中心	1	1
CNCERT 江苏分中心	1	1
CNCERT 天津分中心	1	1
个人	348	348
报送总计	3393	2413

本周漏洞按类型和厂商统计

本周，CNVD 收录了 699 个漏洞。应用程序 329 个，WEB 应用 135 个，智能设备（物联网终端设备）79 个，操作系统 78 个，网络设备（交换机、路由器等网络端设备）

65 个，数据库 7 个，安全产品 6 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	329
WEB 应用	135
智能设备（物联网终端设备）	79
操作系统	78
网络设备（交换机、路由器等网络端设备）	65
数据库	7
安全产品	6

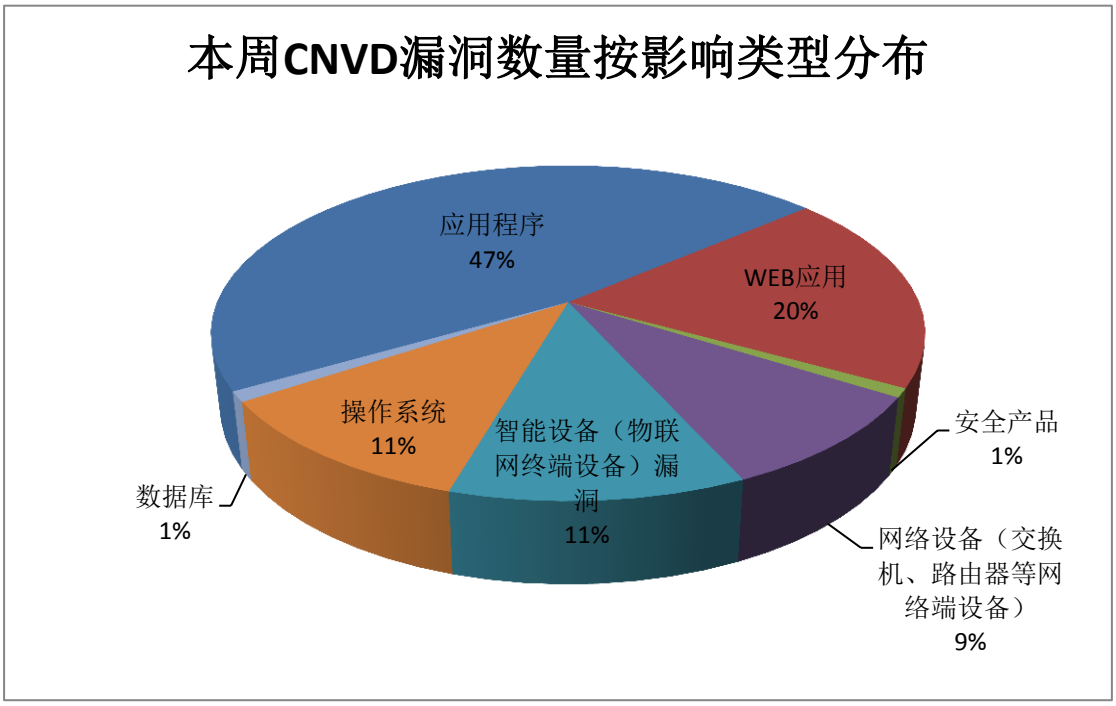

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、IBM、Samsung 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	Microsoft	30	5%
2	IBM	28	4%
3	Samsung	27	4%
4	Apple	36	5%
5	Moxa	23	3%
6	Cisco	21	3%

7	ASUS	19	3%
8	WordPress	17	2%
9	Cloudera	14	2%
10	其他	484	69%

本周行业漏洞收录情况

本周，CNVD 收录了 42 个电信行业漏洞，40 个移动互联网行业漏洞，21 个工控行业漏洞（如下图所示）。其中，“Moxa EDS-G516E 和 EDS-510E series 缓冲区溢出漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-14243）、IBM QRadar Advisor With Watson App 信息泄露漏洞、D-Link DAP-1330 认证绕过漏洞、Cisco SD-WAN Solution 输入验证错误漏洞”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/

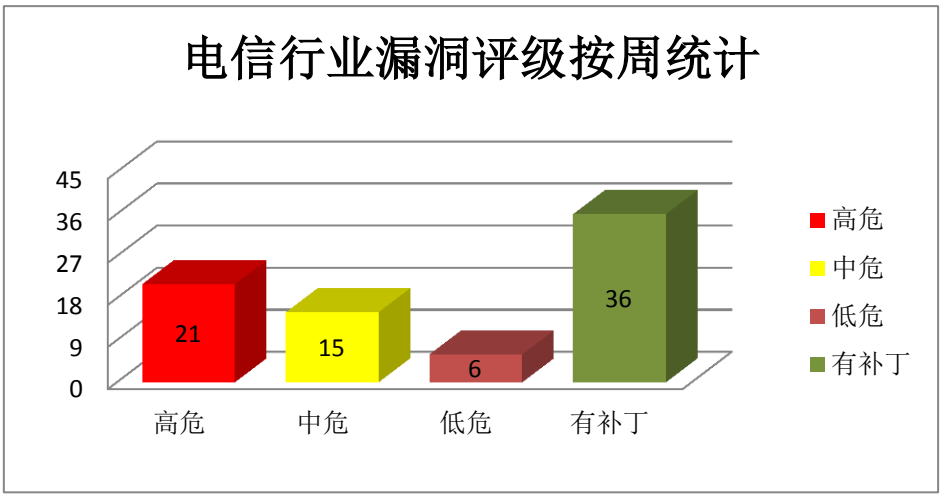

图 3 电信行业漏洞统计

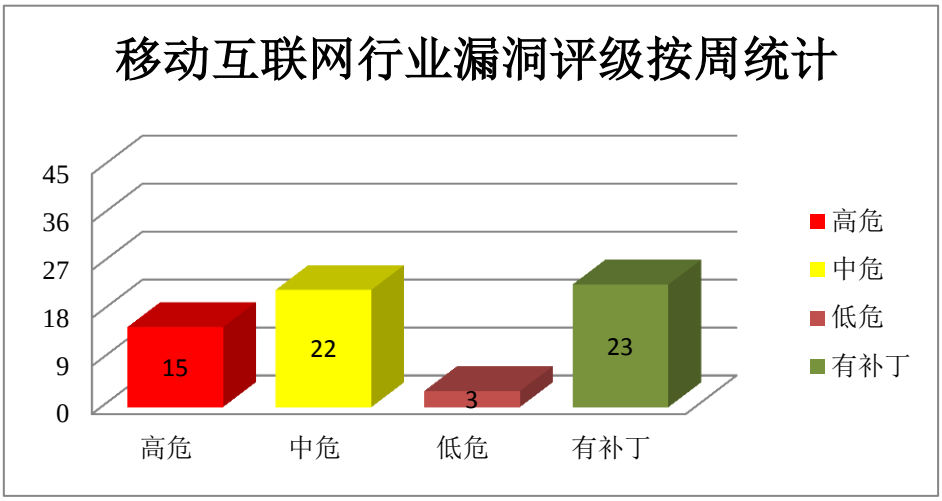

图 4 移动互联网行业漏洞统计

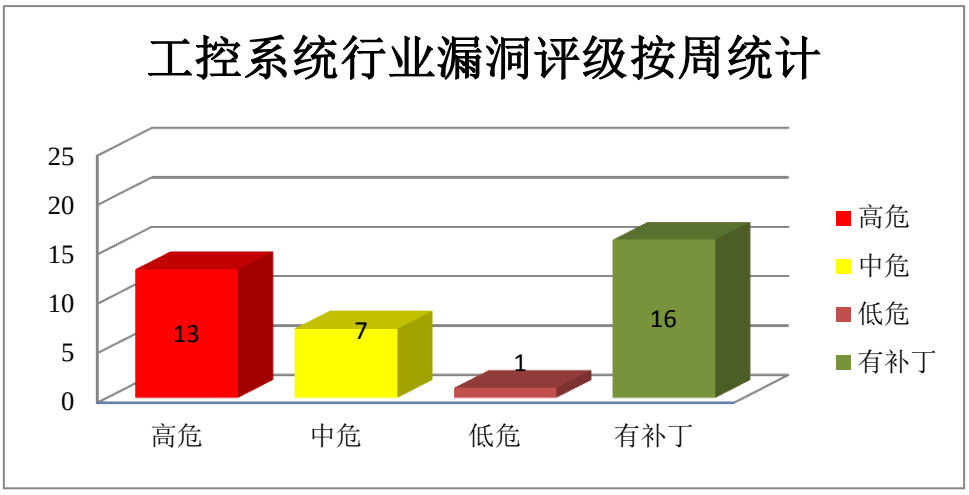

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Emptoris Spend Analysis 是一套采购解决方案中的用于对分散系统的支出数据进行整合、清理和分类的产品。IBM Spectrum Protect Plus 是一套数据保护平台。"IBM QRadar Advisor with Watson 是一套安全威胁分析解决方案。IBM Security Identity Manager（ISIM）是一套身份管理和治理解决方案。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，执行任意命令等。

CNVD 收录的相关漏洞包括：IBM Emptoris Spend Analysis SQL 注入漏洞（CNVD-2020-13057）、IBM Spectrum Protect Plus 命令注入漏洞（CNVD-2020-14207、CNVD-2020-14208、CNVD-2020-14211、CNVD-2020-14212、CNVD-2020-14213）、IBM QRadar Advisor With Watson App 信息泄露漏洞、IBM Security Identity Manager 信任管

理问题漏洞。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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-13057
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14207
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14208
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14211
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14212
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14213
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14323
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14763

2、Apple 产品安全漏洞

Apple Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。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。Apple macOS Catalina 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，攻击者可利用漏洞造成应用程序意外终止或执行任意代码。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-14243、CNVD-2020-14244）、多款 Apple 产品 Core Data 组件和 Siri 组件缓冲区溢出漏洞、多款 Apple 产品 UIFoundation 组件缓冲区溢出漏洞、多款 Apple 产品 Foundation 组件缓冲区溢出漏洞、多款 Apple 产品 Core Data 组件缓冲区溢出漏洞、Apple macOS Catalina 内存破坏漏洞（CNVD-2020-14694、CNVD-2020-14695）。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-2020-14243
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14244
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14259
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14258
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14261
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14688
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14694
https://www.cnvd.org.cn/flaw/show/CNVD-2020-14695

3、Microsoft 产品安全漏洞

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。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft Exchange Server 是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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Microsoft Windows Remote Desktop Client 代码执行漏洞、Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2020-13557、CNVD-2020-13559）、Microsoft Internet Explorer 缓冲区溢出漏洞（CNVD-2020-13691）、Microsoft Exchange 验证密钥远程代码执行漏洞、Microsoft Windows Graphics 组件权限提升漏洞（CNVD-2020-14699）、Microsoft DirectX 权限提升漏洞、Microsoft Windows Win32k 权限提升漏洞（CNVD-2020-14702）。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-2020-13471
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13473
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13475
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13477
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13491
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13492
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13508
https://www.cnvd.org.cn/flaw/show/CNVD-2020-13515

4、Moxa 产品安全漏洞

Moxa AWK-3131A 是一款无线接入设备。Moxa EDS-G516E 和 EDS-510E series 都是 Moxa 生产的以太网交换机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞解密被捕获的流量，绕过身份验证，执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：Moxa AWK-3131A 访问控制错误漏洞、Moxa AWK-3131A 操作系统命令注入漏洞（CNVD-2020-13473）、Moxa AWK-3131A iw_webs 功能操作系统命令注入漏洞（CNVD-2020-13475、CNVD-2020-13477）、Moxa AWK-3131A 身份验证绕过漏洞、Moxa AWK-3131A ServiceAgent 信任管理问题漏洞、Moxa EDS-G516E 和 EDS-510E series 缓冲区溢出漏洞（CNVD-2020-13508、CNVD-2020-13515）。其中，“Lenovo System Interface Foundation 未签名 DLL 加载漏洞、Lenovo XClarity Administrator 访问控制错误漏洞、Lenovo ThinkPad 输入验证错误漏洞、Lenovo System Interface Foundation 任意代码执行漏洞”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-2020-09987
http://www.cnvd.org.cn/flaw/show/CNVD-2020-09984
http://www.cnvd.org.cn/flaw/show/CNVD-2020-09985

http://www.cnvd.org.cn/flaw/show/CNVD-2020-09986

http://www.cnvd.org.cn/flaw/show/CNVD-2020-09988

http://www.cnvd.org.cn/flaw/show/CNVD-2020-10122

http://www.cnvd.org.cn/flaw/show/CNVD-2020-10124

http://www.cnvd.org.cn/flaw/show/CNVD-2020-10123

5、NETGEAR Nighthawk X10-R9000 命令注入漏洞

NETGEAR Nighthawk X10-R9000 是一款无线路由器。本周，NETGEAR Nighthawk X10-R9000 被披露存在命令注入漏洞。攻击者可利用该漏洞执行非法命令。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-2020-13467

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-2020-09966	多款 Qualcomm 产品输入验证错误漏洞（CNVD-2020-09966）	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.qualcomm.com/company/product-security/bulletins/february-2020-bulletin
CNVD-2020-13041	NEC Aterm WG2600HS OS 命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://jvndb.jvn.jp/en/contents/2020/JVNDB-2020-000015.html
CNVD-2020-13043	Progress Software MOVEit Transfer 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://community.ipswitch.com/s/article/MOVEit-Transfer-Security-Vulnerabilities-Feb-2020
CNVD-2020-13161	Linux kernel ‘btrfs_ioctl_space_info’缓冲区溢出漏洞	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.kernel.org/
CNVD-2020-13163	GNU Aspell libaspell.a 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：http://aspell.net/buffer-overread-ucs.txt
CNVD-2020-13183	FasterXML jackson-databind 远程代码执行漏洞	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/FasterXML/jackson-databind/issues/2620
CNVD-2020-	Synacor Zimbra Collaboration	高	目前厂商已发布升级补丁以修复漏

13194	操作系统命令注入漏洞		洞，补丁获取链接：https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories
CNVD-2020-13488	Cisco Unified Contact Center Express 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-privesc-Zd7bvwyf
CNVD-2020-13489	Adobe After Effects 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://helpx.adobe.com/security/products/after_effects/apsb20-09.html
CNVD-2020-13853	HP Access Control 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.hp.com/in-en/document/c06463137
CNVD-2020-13862	Google Chrome speech 资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop_18.html

小结：本周，IBM 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，执行任意命令等此外，Apple、Microsoft、Moxa 等多款产品被披露存在多个漏洞，攻击者可利用漏洞解密被捕获的流量，绕过身份验证，提升权限，执行任意代码或导致拒绝服务等。另外，NETGEAR Nighthawk X10-R9000 被披露存在命令注入漏洞。攻击者可利用该漏洞执行非法命令。

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、Rasilient PixelStor 5000 远程代码执行漏洞

验证描述

Rasilient PixelStor 5000 是一款 RAID 磁盘阵列。

Rasilient PixelStor 5000 K:4.0.1580-20150629（KDI 版）中的 languageOptions.php 存在远程代码执行漏洞。未认证攻击者可通过 lang 参数利用该漏洞远程执行代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/155898/PixelStor-5000-K-4.0.1580-20150629-Remote-Code-Execution.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-14703

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. 新高风险漏洞 Ghostcat 影响 Apache Tomcat 服务器

利用严重漏洞 Ghostcat 可以影响 Apache Tomcat，从服务器读取文件，在某些情况下甚至可以实现远程代码执行。该漏洞被追踪为 CVE-2020-1938，是由中国网络安全公司 Chaitin Tech 的研究人员发现并报告给 Apache 软件基金会的。

参考链接：https://www.securityweek.com/apache-tomcat-affected-serious-ghostcat-vulnerability

2. 黑客在 PayPal 的 Google Pay 集成中发现漏洞，进行未经授权的付款

近日黑客在 PayPal 的 Google Pay 集成中发现了一个漏洞，现在正使用它通过 PayPal 帐户进行未经授权的交易。自上周五以来，用户报告称在其 PayPal 历史中突然出现了源自其 Google Pay 帐户的神秘交易。

参考链接：https://www.cnbeta.com/articles/tech/948363.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