国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 04 月 06 日-2020 年 04 月 12 日　　2020 年第 15 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 415 个，其中高危漏洞 147 个、中危漏洞 232 个、低危漏洞 36 个。漏洞平均分值为 6.05。本周收录的漏洞中，涉及 0day 漏洞 168 个（占 41%），其中互联网上出现“Apache Solr Velocity Template 远程代码执行漏洞、WordPress Randy Peterman Murph StatTraq SQL 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 2497 个，与上周（3567 个）环比减少 30%。

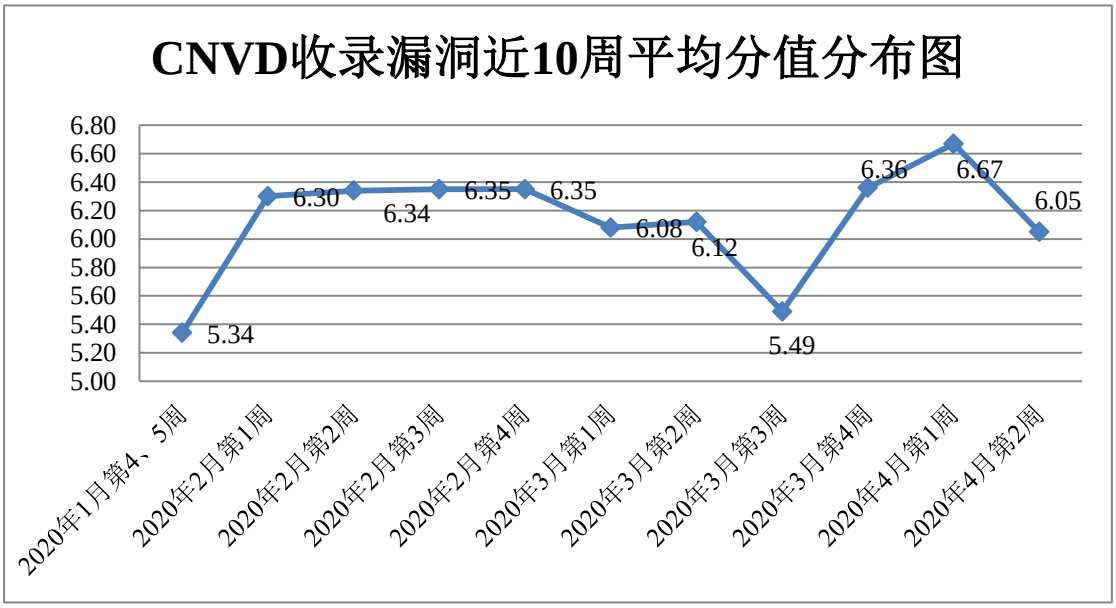

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 33 起，向基础电信企业通报漏洞事件 11 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 278 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 29 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 11 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：

广州市悦阁网络科技有限公司、怀化第五元素网络信息有限公司、上海顶想信息科技有限公司、河南跃龙门科技有限公司、石家庄指南针网络科技有限公司、青岛汇商传媒有限公司、北京良精志诚科技有限责任公司、北京智量科技有限公司、壹拾捌号网络技术有限公司、北京通达信科科技有限公司、西安佰联网络技术有限公司、北京小米科技有限责任公司、深圳市努比亚信息技术有限公司、江苏紫米电子技术有限公司、联想集团、上海分互链信息技术有限公司、广州市璐华计算机有限公司、百硕网络科技有限公司、合肥辉创网络科技有限公司、济南白菜网络技术有限公司、上海商派网络科技有限公司、北京（山东）城通科技有限公司、深圳市贝尔利科技有限公司、廊坊市极致网络科技有限公司、秦皇岛商景科技有限公司、海南易而优科技有限公司、淮南市银泰软件科技有限公司、唐山长城网络有限公司、桂林天生智创信息技术有限公司、普联技术有限公司、深圳市朝恒辉网络科技有限公司、北京国炬信息技术有限公司、长沙米拓信息技术有限公司、北京多点在线科技有限公司、益盟股份有限公司、福州靠谱网络有限公司、上海九方云智能科技有限公司、上海迈微软件科技有限公司、北京猿力教育科技有限公司、广州市智米信息科技有限公司、江西华邦传媒有限公司、北京海腾时代科技有限公司、友讯电子设备（上海）有限公司、海南赞赞网络科技有限公司、上海泛微网络科技股份有限公司、北京杰控科技有限公司、浙江核新同花顺网络信息股份有限公司、北京派网软件有限公司、安阳智道传媒有限公司、北京学而思教育科技有限公司、北京翰博尔信息技术股份有限公司、长沙天二网络科技有限公司、河北唐山长城网络有限公司、漳州豆壳网络科技有限公司、雄帝股份有限公司、中国节能环保集团有限公司、北京康盛新创科技有限责任公司、安徽省科迅教育装备有限公司、中国电力发展促进会、施耐德（Schneider Electric）、思博特科技、伟创互联网络技术开发团队、聚易技术团队、广州畅梦网络、宜软通网、易橙互联、无忧网络、飞飞影视导航系统、梦想 cms、百家 cms、稻草人 cms、海洋 CMS、逍遥 B2C 商城系统、ZZCMS、Anker Technology (UK) Ltd、MOMAX Technology Ltd、YKCMS5、POPOJICMS、BSPHP、pdfresurrect、zzzcms、Catfish CMS、EBCMS、Xnview、YCCMS、HuCart、115CMS、Gridea、iCMS、CIMCO 和 Psi。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、恒安嘉新(北京)科技股份公司、哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、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、长春嘉诚信息技术股份有限公司、河南灵创电子科技有限公司、北京铭图天成信息技术有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、北京机沃科技有限公司、山东云天安全技术有限公司、北京华云安信息技术有限公司、新疆海狼科技有限公司、杭州海康威视数字技术股份有限公司、上海观安信息技术股份有限公司、内蒙古洞明科技有限公司、北京圣博润高新技术股份有限公司、博智安全科技股份有限公司、郑州赛欧思科技有限公司、山东新潮信息技术有限公司、山东云天安全大数据技术有限公司、山石网科通信技术股份有限公司、河北千诚电子科技有限公司、广西网信信息安全等级保护测评有限公司、河南信安世纪科技有限公司、四川哨兵信息科技有限公司、中移（杭州）信息技术有限公司及其他个人白帽子向 CNVD 提交了 2311 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 2497 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
阿里云计算有限公司	940	0
奇安信网神（补天平台）	696	696
斗象科技（漏洞盒子）	675	675
上海交大	395	395
恒安嘉新(北京)科技股份公司	394	0
哈尔滨安天科技集团股份有限公司	186	0
北京天融信网络安全技术有限公司	128	2
华为技术有限公司	122	0
深信服科技股份有限公司	84	0
新华三技术有限公司	74	0
北京启明星辰信息安全技术有限公司	61	10
厦门服云信息科技有限公司	42	0
北京神州绿盟科技有限公司	39	4

北京奇虎科技有限公司	23	0
杭州安恒信息技术股份有限公司	15	15
北京安信天行科技有限公司	6	6
北京知道创宇信息技术股份有限公司	1	0
远江盛邦（北京）网络安全科技股份有限公司	111	111
长春嘉诚信息技术股份有限公司	52	52
河南灵创电子科技有限公司	34	34
北京铭图天成信息技术有限公司	24	24
国瑞数码零点实验室	22	22
内蒙古奥创科技有限公司	18	18
杭州迪普科技股份有限公司	14	0
北京机沃科技有限公司	9	9
山东云天安全技术有限公司	9	9
北京华云安信息技术有限公司	8	8
新疆海狼科技有限公司	8	8
杭州海康威视数字技术股份有限公司	5	5
上海观安信息技术股份有限公司	5	5
内蒙古洞明科技有限公司	4	4
北京圣博润高新技术股份有限公司	3	3
博智安全科技股份有限公司	3	3
郑州赛欧思科技有限公司	3	3
山东新潮信息技术有限公司	2	2

山东云天安全大数据技术有限公司	2	2
山石网科通信技术股份有限公司	2	2
河北千诚电子科技有限公司	1	1
广西网信信息安全等级保护测评有限公司	1	1
河南信安世纪科技有限公司	1	1
四川哨兵信息科技有限公司	1	1
中移（杭州）信息技术有限公司	1	1
CNCERT 天津分中心	20	20
CNCERT 四川分中心	5	5
CNCERT 西藏分中心	5	5
CNCERT 河北分中心	3	3
CNCERT 海南分中心	2	2
CNCERT 宁夏分中心	1	1
个人	329	329
报送总计	4589	2497

本周漏洞按类型和厂商统计

本周，CNVD 收录了 415 个漏洞。应用程序 236 个，WEB 应用 94 个，操作系统 28 个，安全产品 21 个，网络设备（交换机、路由器等网络端设备）20 个，智能设备（物联网终端设备）13 个，数据库 3 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	236
WEB 应用	94
操作系统	28
安全产品	21

网络设备（交换机、路由器等网络端设备）	20
智能设备（物联网终端设备）	13
数据库	3

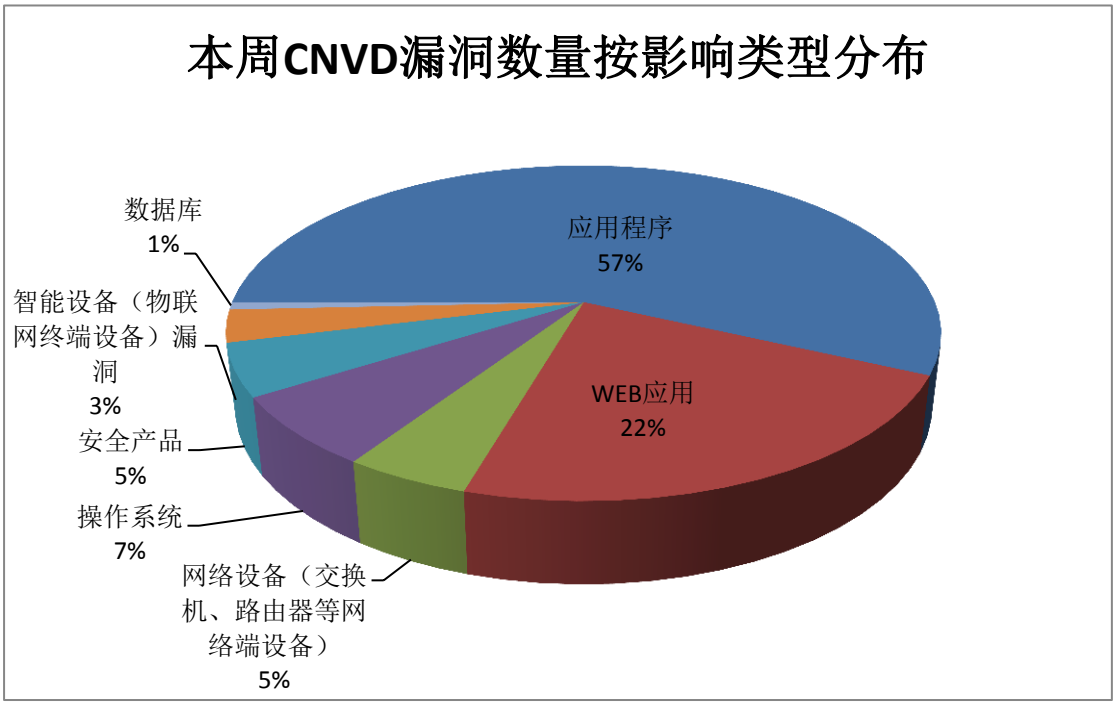

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、IBM、GitLab 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	Apple	18	4%
2	IBM	17	4%
3	GitLab	16	4%
4	Huawei	16	4%
5	CIPPlanner	13	3%
6	Advantech	9	2%
7	Avast	9	2%
8	Pulse Secure	9	2%
9	ASUS	8	2%
10	其他	300	73%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，28 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Google Android Framework 权限提升漏洞（CNVD-2020-22161）、ASUS SmartHome 访问控制错误漏洞、多款 Apple 产品 IOHIDFamily 组件缓冲区溢出漏洞、GE CIMPLICITY 权限提升漏洞”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/

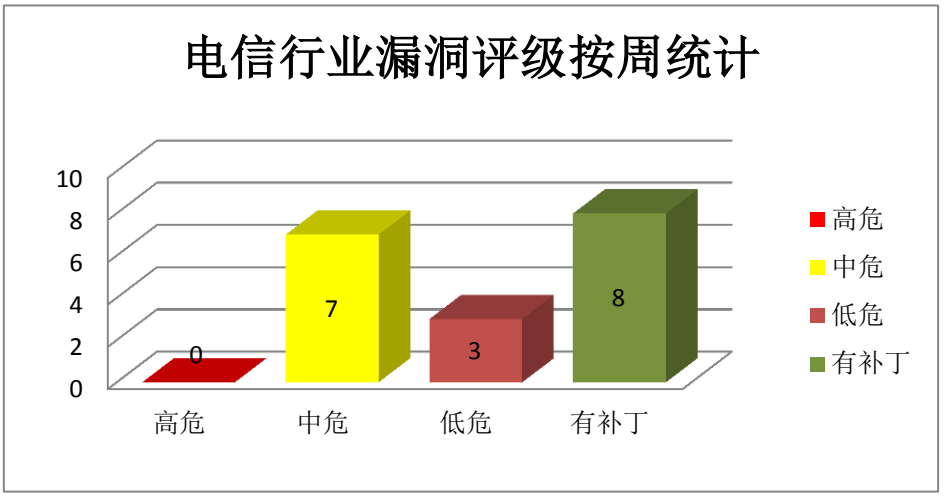

图 3 电信行业漏洞统计

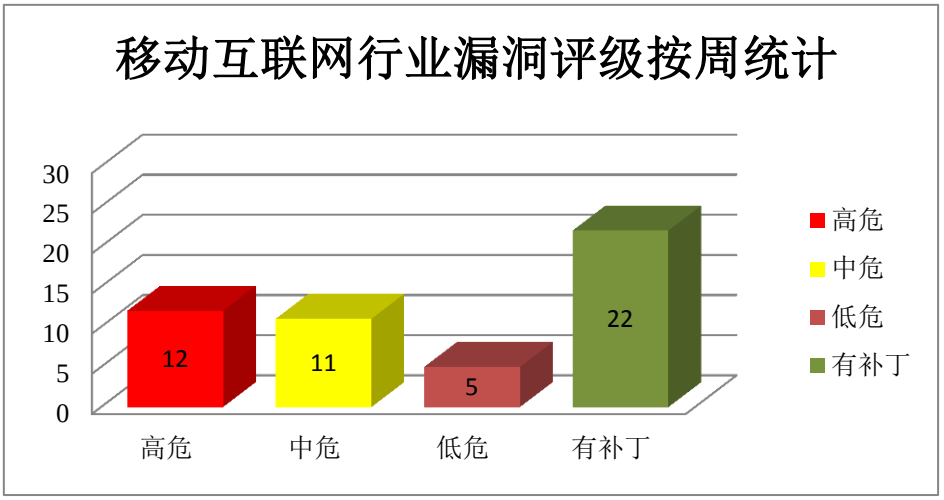

图 4 移动互联网行业漏洞统计

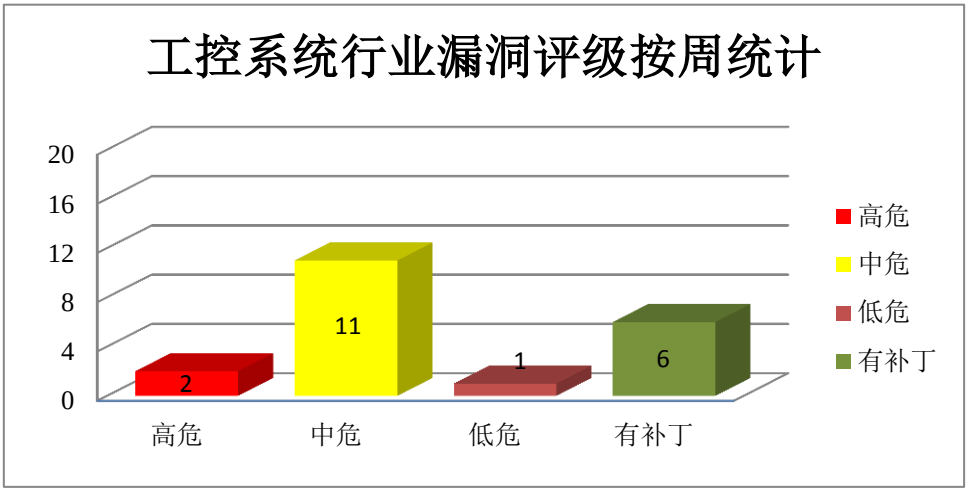

图 5 工控系统行业漏洞统计

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、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 watchOS 是一套智能手表操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：多款 Apple 产品 Kernel 组件内存破坏漏洞（CNVD-2020-22118、CNVD-2020-22133、CNVD-2020-22132）、多款 Apple 产品 Image Processing 组件资源管理错误漏洞、多款 Apple 产品 IOHIDFamily 组件缓冲区溢出漏洞、多款 Apple 产品 WebKit 组件类型混淆漏洞（CNVD-2020-22129）、多款 Apple 产品 WebKit 组件内存消耗漏洞、多款 Apple 产品 libxml2 组件缓冲区溢出漏洞（CNVD-2020-22134）。其中，除“多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-22132）”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-2020-22118

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22121

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22120

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22129

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22128

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22133

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22132

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22134

2、Huawei 产品安全漏洞

Huawei USG9500 等都是中国华为（Huawei）公司的产品。USG9500 是一款数据中心防火墙产品。NIP6800 是一套入侵防御系统。USG6600 是一款数据中防火墙产品。Huawei Mate 20、Mate 30 和 Mate 30 Pro 都是中国华为（Huawei）公司的一款智能手机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行未授权操作，获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei Mate 20 和 Mate 30 Pro 授权问题漏洞、Huawei NIP6800、Secospace USG6600 和 USG9500 无效指针访问漏洞（CNVD-2020-22007）、Huawei NIP6800、Secospace USG6600 和 USG9500 资源管理错误漏洞、Huawei NIP6800、Secospace USG6600 和 USG9500 访问控制绕过漏洞、Huawei NIP6800，Secospace USG6600 和 USG9500 越界写入漏洞、Huawei NIP6800、Secospace USG6600 和 USG9500 越界读取漏洞、Huawei NIP6800、Secospace USG6600 和 USG9500 拒绝服务漏洞（CNVD-2020-22011）、Huawei Mate 30 Pro 和 Huawei Mate 30 授权问题漏洞。其中，“Huawei NIP6800、Secospace USG6600 和 USG9500 越界读取漏洞”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-2020-22002
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22007
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22006
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22005
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22004
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22009
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22011
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22206

3、IBM 产品安全漏洞

IBM Security Information Queue 是一款数据集成产品。IBM Aspera 是一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。IBM WebSphere Application Server Liberty 是一款构建于 Open Liberty 项目之上的 Java 应用程序服务器。IBM Rational Quality Manager（RQM）是一套协作的、基于 Web 的质量管理解决方案。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，执行客户端代码。

CNVD 收录的相关漏洞包括：IBM Security Information Queue 信息泄露漏洞（CNVD-2020-22186、CNVD-2020-22189、CNVD-2020-22188、CNVD-2020-22187）、多款 IBM 产品缓冲区溢出漏洞（CNVD-2020-22192）、IBM WebSphere Application Server Liberty 跨站脚本漏洞（CNVD-2020-22194、CNVD-2020-22193）、IBM Rational Quality Manager 信息泄露漏洞（CNVD-2020-22336）。其中“多款 IBM 产品缓冲区溢出漏洞（CNVD-2020-22192）”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-2020-22186

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22189

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22188

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22187

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22192

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22194

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22193

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22336

4、GitLab 产品安全漏洞

GitLab 是一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行未授权访问，获取敏感信息等。

CNVD 收录的相关漏洞包括：GitLab 信息泄露漏洞（CNVD-2020-22022、CNVD-2020-22024）、GitLab 竞争条件漏洞、GitLab 资源管理问题漏洞、GitLab EE/CE 信息泄露漏洞（CNVD-2020-22238、CNVD-2020-22242、CNVD-2020-22239）、GitLab EE/CE SSRF 漏洞。其中，“GitLab EE/CE SSRF 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-2020-22022

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22021

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22025

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22024

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22238

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22242

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22239

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22243

5、D-Link DIR-615 授权问题漏洞

D-Link DIR-615 是一款无线路由器。本周，D-Link DIR-615 被披露存在授权问题漏洞。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。攻击者可利用该漏洞修改页面的数据字段。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-2020-22295

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-2020-21803	Mozilla Firefox 和 Firefox ESR 内存错误引用漏洞（CNVD-2020-21803）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/
CNVD-2020-21911	Apache Traffic Server 环境问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread.html/r99d18d0bc4daa05e7d0e5a63e0e22701a421b2ef5a8f4f7694c43869%40%3Cannounce.trafficserver.apache.org%3E
CNVD-2020-22212	多款 Fortinet 产品资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/psirt/FG-IR-19-013
CNVD-2020-22303	ASUS SmartHome 访问控制错误漏洞	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.asus.com
CNVD-2020-22310	Advantech WebAccess/NMS 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.advantech.com/
CNVD-2020-22318	GE CIMPLICITY 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://digitalsupport.ge.com
CNVD-2020-22316	Advantech WebAccess/NMS SQL 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.advantech.com/
CNVD-2020-22345	Geutebrück G-Cam 和 G-Code OS 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://ics-cert.us-cert.gov/advisories/ICSA-19-155-03
CNVD-2020-22352	SaltStack Salt MySQL 模块 SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ShantonRU/salt/commit/a46c86a987c78e74e87969d8d3b27094e6544b7a
CNVD-2020-22378	Mitsubishi FR Configurator2 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitsubishielectric.com/

小结：本周，Apple 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，或导致应用程序崩溃。此外 Huawei、IBM、GitLab 等多款产品被披露存在多个漏洞，

攻击者可利用漏洞执行未授权操作，获取敏感信息，导致拒绝服务等。另外，D-Link DIR-615 被披露存在授权问题漏洞。攻击者可利用该漏洞修改页面的数据字段。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、Apache Solr Velocity Template 远程代码执行漏洞

验证描述

Apache Solr 是美国阿帕奇（Apache）软件基金会的一款基于 Lucene（一款全文搜索引擎）的搜索服务器。该产品支持层面搜索、垂直搜索、高亮显示搜索结果等。

Apache Solr Velocity Template 存在远程代码执行漏洞，该漏洞源于程序未能正确地验证用户提交的数据。远程攻击者可通过发送恶意的 HTTP 请求利用该漏洞在底层操作系统上执行任意代码。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2020040008

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-21800

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. 深信服 VPN 设备漏洞被黑客组织利用，针对我国驻外机构及部分政府单位（附完整修复方案）

近日，深信服 SSL VPN 设备被曝存在漏洞，APT 组织 Darkhotel（APT-C-06）利用该组织对我国多驻外机构发起攻击，甚至近期已经开始针对北京、上海等地政府相关机构。根据深信服官网的产品信息，其 SSL VPN 客户端并发授权已累计使用超过 260 万个，服务于全国 18000 多家各行业客户，并且入围了中央政府、国税总局、建设银行、中国移动、联通集团等高端行业的采购清单。

这既是产品实力体现，但也同时承担着相应的安全压力。一旦出现重大漏洞，影响范围也是非常巨大。于是在 4 月 3 日收到漏洞报告之后，深信服紧急发布 SSL VPN 产

品修复补丁，完成全面安全风险排查，并且在第一时间发布安全公告公布详细的修复方案。

参考链接：https://www.freebuf.com/news/232618.html

2. 旧金山机场遭网络攻击已确认：用户 Windows 密码被盗

黑客在网络攻击期间设法破坏了旧金山国际机场的两个网站：SFOConnect.com 和 SFOConstruction.com，并可能窃取了用户的 Windows 登录凭据。

参考链接：https://www.forbes.com/sites/daveywinder/2020/04/11/san-francisco-airport-cyber-attack-confirmed-windows-passwords-stolen/#5bf1667225b9

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