国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 07 月 20 日-2020 年 07 月 26 日　　2020 年第 30 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 481 个，其中高危漏洞 147 个、中危漏洞 290 个、低危漏洞 44 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 204 个（占 42%），其中互联网上出现“Open eClass SQL 注入漏洞、Exhibitor 命令注入漏洞”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 3433 个，与上周（3700 个）环比减少 7%。

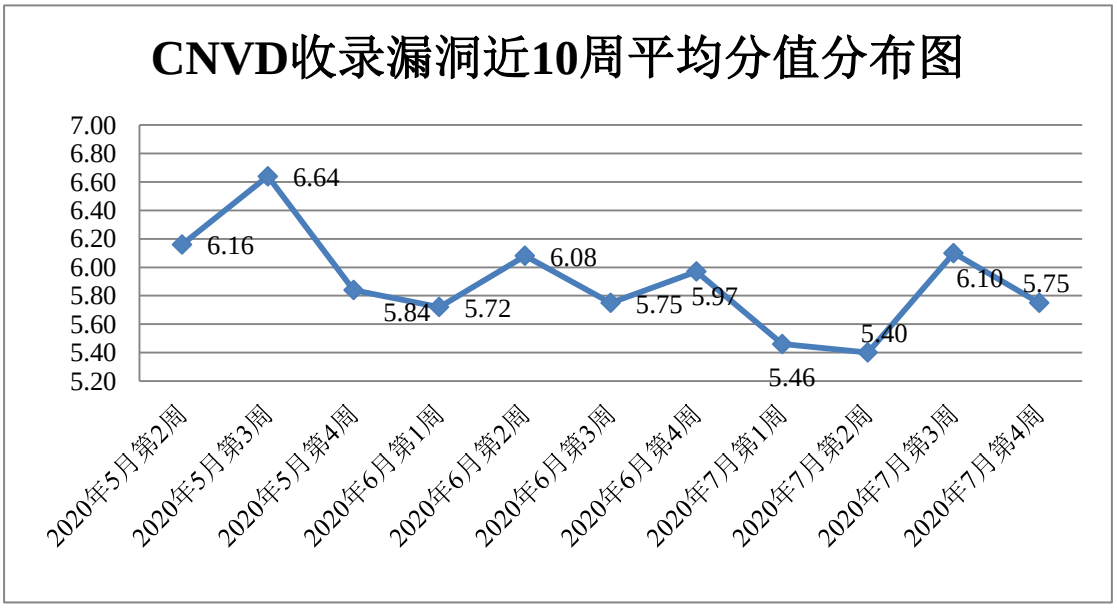

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 1 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 465 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 57 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：

成都奥科睿科技有限公司、海南易而优科技有限公司、铭飞科技有限公司、邳州天目网络科技有限公司、安徽科迅教育装备集团有限公司、郑州谷赛网络科技有限公司、重庆逐越光电科技有限公司、中新网络信息安全股份有限公司、上海丹帆网络科技有限公司、深圳市博思协创网络科技有限公司、河南青峰网络科技有限公司、深圳市步科电气有限公司、西门子（中国）有限公司、国晋信息科技有限公司、合肥蓝领商务信息有限公司、上海卓卓网络科技有限公司、石家庄市征红网络科技有限公司、北京良精志诚科技有限责任公司、安阳智道传媒有限公司、北京用友政务软件股份有限公司、上海亿速网络科技有限公司、诸城三剑网络传媒有限公司、珠海金山办公软件有限公司、深圳市索爱智能科技有限公司、北京通达信科科技有限公司、洪湖尔创网联信息技术有限公司、海南赞赞网络科技有限公司、上海金电网安科技有限公司、北京网康科技有限公司、石家庄和嘉科技有限公司、福建省海峡信息技术有限公司、北京维方通信息技术有限公司、厦门优莱柏网络科技有限公司、长沙网久软件有限公司、鞍山光武网络科技有限公司、常州遨翔网络科技有限公司、北京理正软件股份有限公司、浙江逆天网络科技有限责任公司、济南亘安信息技术有限公司、深圳市时代映像文化传媒有限公司、浙江永拓信息科技有限公司、深圳市天地心网络技术有限公司、东方博冠（北京）科技有限公司、哈尔滨伟成科技有限公司、瑞芯微电子股份有限公司、四川省安全科学技术研究院、广西感知物联科技有限公司、中兴保全股份有限公司、南京铁行网络科技有限公司、北京华清信安科技有限公司、南昌腾速科技有限公司、浙江慕枫网络科技有限公司、深圳锐取信息技术股份有限公司、青岛商至信网络科技有限公司、苏州互众网络技术有限公司、南昌市博然科技有限公司、青岛自动化仪表有限公司、湖南翱云网络科技有限公司、郑州壹网无忧信息技术有限公司、廊坊市商昊信息网络有限公司、合肥天寻信息科技有限公司、上海孚盟软件有限公司、桂林佳朋信息科技有限公司、上海品划网络科技有限公司、中国知网电子杂志社有限公司、普联技术有限公司、上海商派网络科技有限公司、锦江国际酒店管理有限公司、天津南大通用数据技术股份有限公司、鸿宇科技有限公司、中国知网、信呼、施耐德（Schneider Electric）、DM 建站系统、Showdoc、beescms、ZZCMS 和 YzmCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京数字观星科技有限公司、华为技术有限公司、深信服科技股份有限公司、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。国瑞数码零点实验室、北京云科安信科技

有限公司、长春嘉诚信息技术股份有限公司、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 、南京众智维信息科技有限公司、山东道普测评技术有限公司、杭州迪普科技股份有限公司、北京华云安信息技术有限公司、山东云天安全技术有限公司、北京禹宏信安科技有限公司、北京天地和兴科技有限公司、山东华鲁科技发展股份有限公司、泽鹿安全、上海纽盾科技股份有限公司、奇安信科技集团股份有限公司、上海观安信息技术股份有限公司、京东云安全、河南信安世纪科技有限公司、北京安华金和科技有限公司、四川赛闯检测股份有限公司、广州安亿信软件科技有限公司、北京浩瀚深度信息技术股份有限公司、广州市蓝爵计算机科技有限公司、北京智游网安科技有限公司、四川哨兵信息科技有限公司及其他个人白帽子向CNVD提交了3433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 2323 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）	968	968
斗象科技（漏洞盒子）	874	874
哈尔滨安天科技集团股份有限公司	596	0
上海交大	481	481
北京数字观星科技有限公司	300	0
华为技术有限公司	152	0
深信服科技股份有限公司	145	0
北京神州绿盟科技有限公司	90	1
北京天融信网络安全技术有限公司	87	15
北京启明星辰信息安全技术有限公司	43	1
西安四叶草信息技术有限公司	26	26
中国电信集团系统集成有限责任公司	20	20
新华三技术有限公司	19	0
沈阳东软系统集成工程有限公司	4	4

恒安嘉新(北京)科技股份公司	3	3
北京安信天行科技有限公司	2	2
北京知道创宇信息技术股份有限公司	1	0
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
国瑞数码零点实验室	241	241
北京云科安信科技有限公司	158	158
长春嘉诚信息技术股份有限公司	83	83
远江盛邦（北京）网络安全科技股份有限公司	67	67
河南灵创电子科技有限公司	24	24
南京众智维信息科技有限公司	22	22
山东道普测评技术有限公司	17	17
杭州迪普科技股份有限公司	16	0
北京华云安信息技术有限公司	9	9
山东云天安全技术有限公司	8	8
北京禹宏信安科技有限公司	7	7
北京天地和兴科技有限公司	6	6
山东华鲁科技发展股份有限公司	6	6
泽鹿安全	6	6
上海纽盾科技股份有限公司	4	4
奇安信科技集团股份有限公司	3	3
上海观安信息技术股份有限公司	3	3
京东云安全	2	2

河南信安世纪科技有限公司	2	2
北京安华金和科技有限公司	2	2
四川赛闯检测股份有限公司	2	2
广州安亿信软件科技有限公司	2	2
北京浩瀚深度信息技术股份有限公司	1	1
广州市蓝爵计算机科技有限公司	1	1
北京智游网安科技有限公司	1	1
四川哨兵信息科技有限公司	1	1
CNCERT 四川分中心	4	4
CNCERT 贵州分中心	1	1
CNCERT 山西分中心	1	1
CNCERT 西藏分中心	1	1
个人	352	352
报送总计	4865	3433

本周漏洞按类型和厂商统计

本周，CNVD 收录了 481 个漏洞。应用程序 200 个，WEB 应用 179 个，操作系统 36 个，数据库 32 个，网络设备（交换机、路由器等网络端设备）29 个，安全产品 3 个，智能设备（物联网终端设备）2 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	200
WEB 应用	179
操作系统	36
数据库	32
网络设备（交换机、路由器等网络端设备）	29
安全产品	3
智能设备（物联网终端设备）漏洞	2

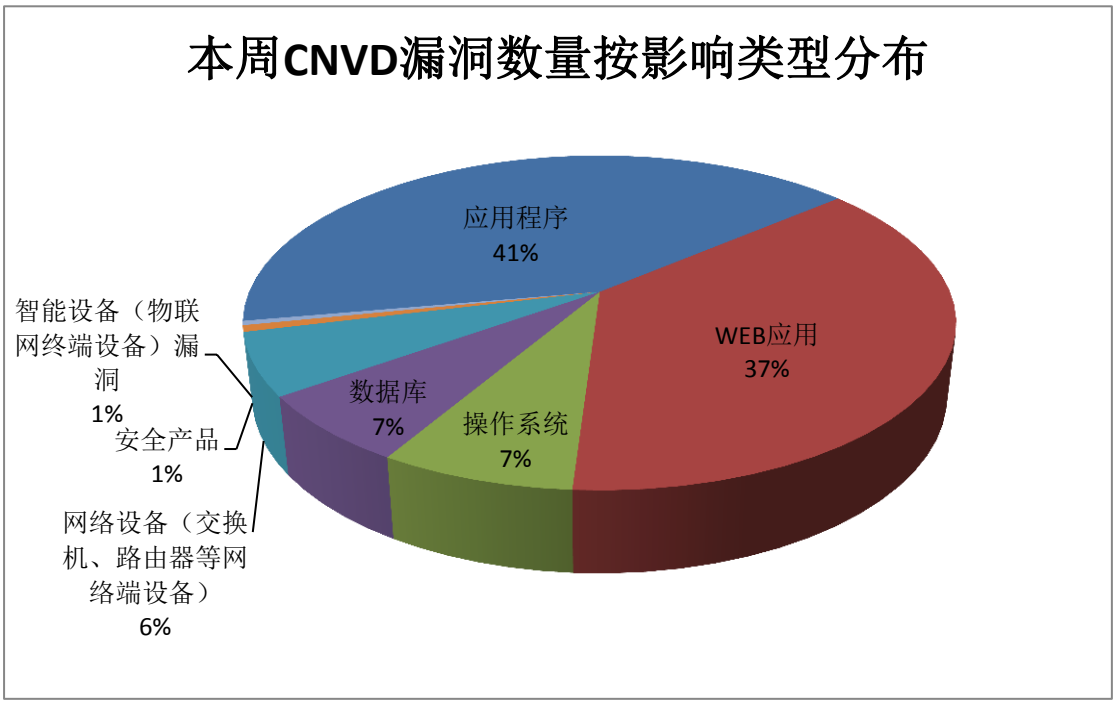

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Mattermost、Microsoft 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	49	10%
2	Mattermost	31	7%
3	Microsoft	23	5%
4	Google	13	3%
5	SAP	11	2%
6	Adobe	10	2%
7	Apache	10	2%
8	Cisco	10	2%
9	Mozilla	9	2%
10	其他	315	65%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，16 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-41233）、

Apple iOS、macOS Mojave 和 tvOS 802.1X 组件输入验证错误漏洞”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/

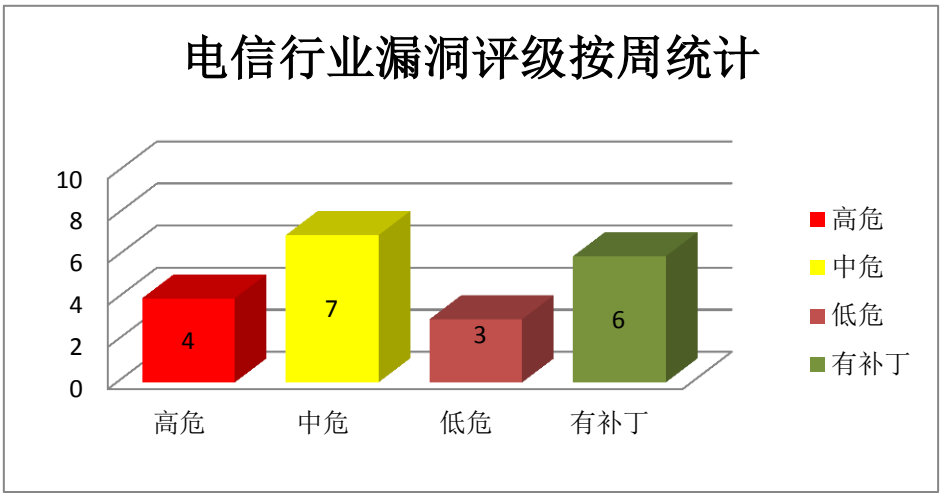

图 3 电信行业漏洞统计

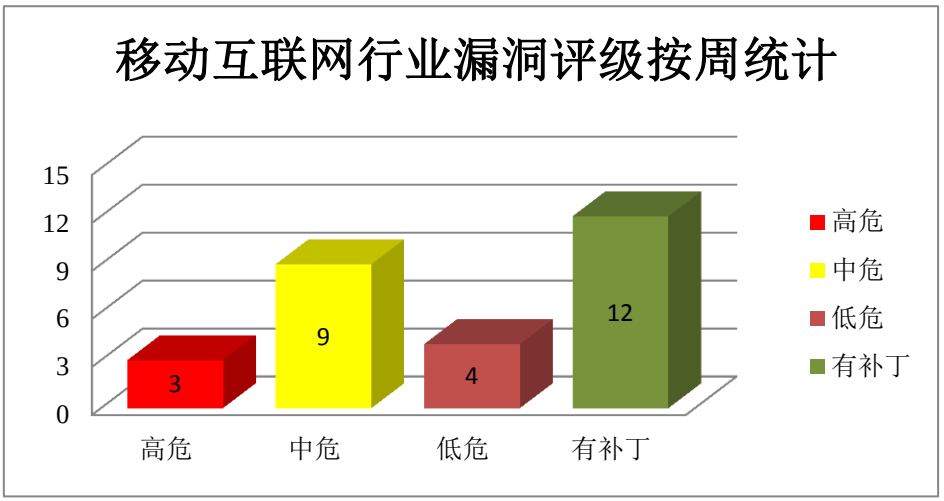

图 4 移动互联网行业漏洞统计

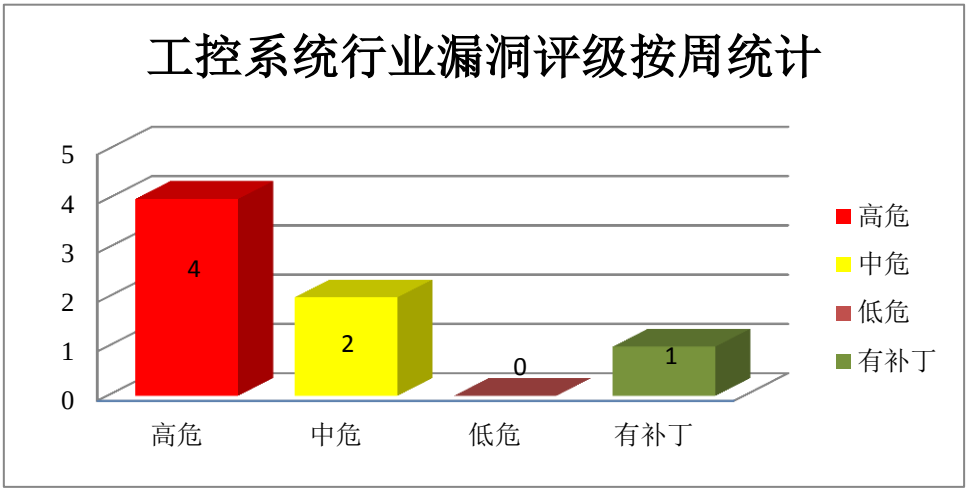

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。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 Excel 是一款 Office 套件中的电子表格处理软件。Microsoft Visual Studio Code 是的一款开源的代码编辑器。Microsoft OneDrive 是一款云备份应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞创建管理员账户，获取权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows Runtime 权限提升漏洞（CNVD-C-2020-159267、CNVD-C-2020-159268、CNVD-2020-40883）、Microsoft Windows 远程代码执行漏洞（CNVD-2020-40876）、Microsoft Remote Desktop Client 远程代码执行漏洞、Microsoft Excel 缓冲区溢出漏洞（CNVD-2020-41714）、Microsoft Visual Studio Code ESLint Extention 命令注入漏洞、Microsoft OneDrive 提权漏洞。其中，除 “Microsoft Windows Runtime 权限提升漏洞（CNVD-C-2020-159267、CNVD-C-2020-159268、CNVD-2020-40883）”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-2020-40874

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40873

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40876

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40881

https://www.cnvd.org.cn/flaw/show/CNVD-2020-40883

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41714

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41742

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41856

2、SAP 产品安全漏洞

SAP Business Client 是德国思爱普（SAP）公司的一款用户界面客户端程序。SAP Business Objects Business Intelligence Platform 是一套商业智能软件和企业绩效解决方案套件。SAP Master Data Governance 是一套用于维护、验证和分发主数据的数据管理工具。SAP Netweaver 是一套面向服务的集成化应用平台。SAP Process Integration 是一种中间件，可使 SAP 与公司中的非 SAP 应用程序或公司外部的系统进行无缝集成。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞登录中央管理控制台，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：SAP Business Client 代码问题漏洞、SAP Business Objects Business Intelligence Platform 访问控制错误漏洞、SAP Master Data Governance SQL 注入漏洞、SAP NetWeaver AS ABAP 和 ABAP Platform 信息泄露漏洞、SAP Business Objects Business Intelligence Platform 跨站脚本漏洞（CNVD-2020-41739、CNVD-2020-41879）、SAP Process Integration PI Rest Adapter 跨站脚本漏洞、SAP Netweaver 路径遍历漏洞。其中，“SAP Business Objects Business Intelligence Platform 访问控制错误漏洞”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-41185

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41542

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41715

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41737

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41739

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41879

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41878

https://www.cnvd.org.cn/flaw/show/CNVD-2020-42019

3、Cisco 产品安全漏洞

Cisco RV110W Wireless-N VPN Firewall 是美国思科（Cisco）公司的一款企业级路由器。Cisco RV340 Dual WAN Gigabit VPN Router 是一款小型 VPN 设备。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。Cisco Vision Dynamic Signage Director 是一套端到端的动态标牌和 IPTV 解决方案。Cisco SD-WAN vEdge 5000 Series Routers 是 SD-WAN 解决方案路由设备。Cisco Enterprise NFV Infrastructure Software（NFVIS）是一套 NVF 基础架构软件平台。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敏感信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-41233）、多款 Cisco 产品任意代码执行漏洞、Cisco SD-WAN vManage Software XML 外部实体注入漏洞、Cisco Vision Dynamic Signage Director SQL 注入漏洞、Cisco SD-WAN vEdge 5000 Series Routers 和 SD-WAN vEdge Cloud Router 拒绝服务漏洞、Cisco Enterprise NFV Infrastructure Software 路径遍历漏洞（CNVD-2020-41804）、Cisco SD-WAN vManage Software SQL 注入漏洞、Cisco SD-WAN vManage Software 后置链接漏洞。其中，除“Cisco SD-WAN vManage Software SQL 注入漏洞、Cisco SD-WAN vManage Software 后置链接漏洞”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-2020-41233
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41232
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41237
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41236
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41235
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41804
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41861
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42251

4、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全功能，执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：多款 Adobe 产品安全绕过漏洞（CNVD-2020-41473、CNVD-2020-41472、CNVD-2020-41474、CNVD-2020-41475）、多款 Adobe 产品越界写入漏洞（CNVD-2020-41476、CNVD-2020-41477）、多款 Adobe 产品空指针漏洞、Adobe Acrobat 和 Reader 存在逻辑缺陷漏洞。其中，“Adobe Acrobat 和 Reader 存在逻辑缺陷漏洞”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-2020-41473
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41472
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41474
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41476
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41475
https://www.cnvd.org.cn/flaw/show/CNVD-2020-41477

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41480

https://www.cnvd.org.cn/flaw/show/CNVD-2020-41875

5、Apache Kylin SQL 注入漏洞

Apache Kylin 是美国阿帕奇（Apache）软件基金会的一款开源的分布式分析型数据仓库。该产品主要提供 Hadoop/Spark 之上的 SQL 查询接口及多维分析（OLAP）等功能。本周，Apache Kylin 被披露存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 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-2020-41857

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-2020-38218	rConfig SQL 注入漏洞（CNVD-2020-38218）	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.rconfig.com/
CNVD-2020-41071	Mozilla Firefox 缓冲区溢出漏洞（CNVD-2020-41071）	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/mfsa2020-20/
CNVD-2020-41086	Fortinet FortiAP-S、FortiAP-W2 和 FortiAP-U 输入验证错误漏洞	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-19-298
CNVD-2020-41502	Apache Camel RabbitMQ 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://camel.apache.org/security/CVE-2020-11972.html
CNVD-2020-41514	MetInfo 存在命令执行漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.mituo.cn/
CNVD-2020-41540	Palo Alto Networks PAN-OS 授权问题漏洞（CNVD-2020-41540）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.paloaltonetworks.com/CVE-2020-2018
CNVD-2020-41590	Pixie 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/usmanhalalit/pixie/commit/9bd991021abbcbfb19347a07dca8b7e518b8abc9

CNVD-2020-41589	ioBroker.admin 目录遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ioBroker/ioBroker.admin/commit/16b2b325ab47896090bc7f54b77b0a97ed74f5cd
CNVD-2020-41778	多款 Qualcomm 产品资源管理错误漏洞（CNVD-2020-41778）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.qualcomm.com/company/product-security/bulletins/january-2020-bulletin
CNVD-2020-41815	Zoom IT installer 未授权操作漏洞	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.zoom.us/hc/en-us/articles/360043036451-Security-CVE-2020-11443
CNVD-2020-42243	Linux kernel 锁定和安全启动限制绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.7.7

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞创建管理员账户，获取权限，执行任意代码等。此外，SAP、Cisco、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全功能，获取敏感信息，执行任意代码，导致拒绝服务等。另外，Apache Kylin 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行非法 SQL 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、Open eClass SQL 注入漏洞

验证描述

Open eClass（前称 GUnet eClass）是希腊 Open eClass 公司的一套完整的课程管理系统。该系统支持用于存储和呈现教材以及异步电子学习服务等。

Open eClass 存在 SQL 注入漏洞。攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：http://target.com/modules/auth/opencourses.php?fc=x[SQL_Injection]

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-41867

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. Citrix Workspace 漏洞可致设备遭受远程入侵

Citrix 修复了 Citrix Workspace 应用程序中的一个漏洞。本地攻击者可以利用该漏洞来提升特权，远程攻击者也可对受影响的设备执行任意命令。

参考链接：https://securityaffairs.co/wordpress/106232/hacking/citrix-workspace-flaw.html

2. Adobe 修复了 Bridge，Photoshop 和 Prelude 产品中的关键代码执行缺陷

Adobe 已发布了针对 Adobe Bridge（APSB20-44），Adobe Photoshop（APSB20-45），Adobe Prelude（APSB20-46）和 Adobe Reader Mobile（APSB20-50）产品中的几个关键代码执行漏洞。Adobe 建议用户按照公告中引用的说明将其产品安装更新到最新版本。

参考链接：https://securityaffairs.co/wordpress/106213/security/adobe-photoshop-bridge-prelude-flaws.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