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 06 日-2020 年 07 月 12 日　　2020 年第 28 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 252 个，其中高危漏洞 56 个、中危漏洞 163 个、低危漏洞 33 个。漏洞平均分值为 5.40。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 17%），其中互联网上出现“ZyXEL Armor X1 WAP6806 路径遍历漏洞、QuickBox 远程代码执行漏洞”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 4971 个，与上周（2924 个）环比增加 70%。

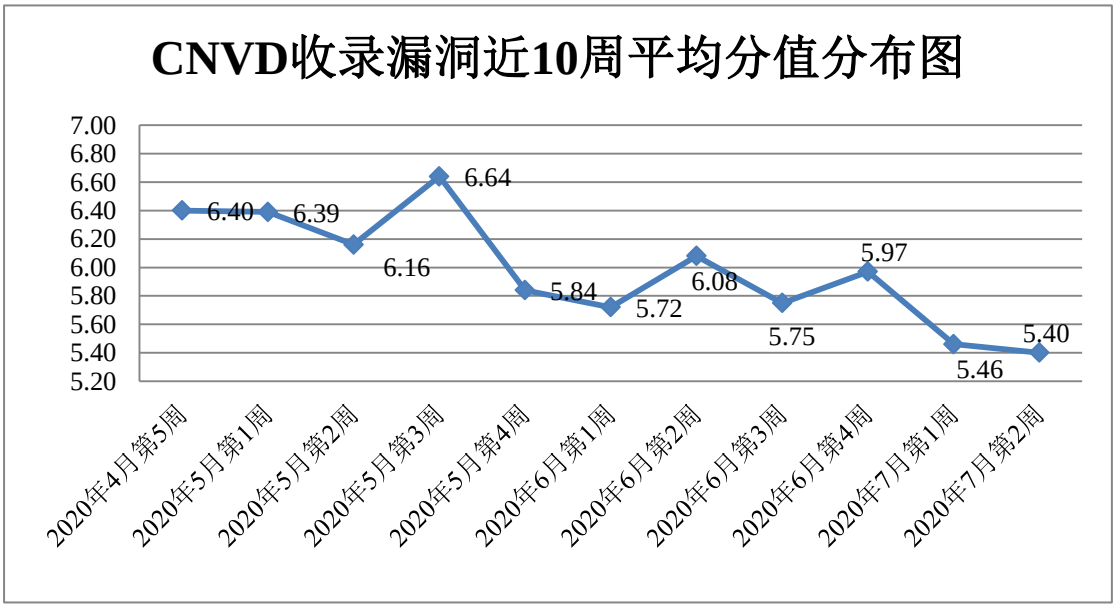

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 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 423 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 50 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 31 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：

北京神州北极科技有限公司、北京米尔伟业科技有限公司、江苏图星软件科技有限责任公司、北京东土科技股份有限公司、茉柏枘（上海）软件科技有限公司、深圳市圆梦云科技有限公司、上海商派网络科技有限公司、厦门二五八网络科技集团股份有限公司、山东农友软件有限公司、浙江大华技术股份有限公司、淄博闪灵网络科技有限公司、河南中钰网络科技有限公司、萍乡市赣西网络科技有限公司、龙采科技集团有限责任公司、深圳齐心好视通云计算有限公司、成都万江港利科技股份有限公司、宜兴市鼎网网络服务有限公司、宜兴易发网络服务有限公司、合肥蓝领商务信息有限公司、四平市九州易通科技有限公司、济南爱程网络科技有限公司、深圳市矽伟智科技有限公司、北京万维盈创科技发展有限公司、新昌县金戈网络有限公司、常州遨翔网络科技有限公司、石家庄百成网络科技有限公司、广州盈可视电子科技有限公司、海南赞赞网络科技有限公司、江苏三恒科技股份有限公司、长沙友点软件科技有限公司、北京惠朗时代科技有限公司、上海品划网络科技有限公司、海南易而优科技有限公司、济南亘安信息技术有限公司、北京良精志诚科技有限责任公司、漳州豆壳网络科技有限公司、深圳市锟铻科技有限公司、广东锜泰电子商务科技有限公司、汕头市盛大文化传播有限公司、上海市企炬企业发展有限公司、四川迅睿云软件开发有限公司、长沙米拓信息技术有限公司、上海布雷德网络科技、中国电源学会、中国教育技术协会、上海荃路软件开发工作室、携程旅行网、剑鱼论坛、魔方动力、中国农业机械化科学研究院、中国运载火箭技术研究院、中国水产科学研究院东海水产研究所、中国医学科学院医学生物学研究所、中国知网、若依、海洋 CMS、通达 CMS、苹果 CMS、YZMCMS、ZZCMS、NiterForum、uublog 和 emlog。

本周，CNVD 发布了《关于 F5 BIG-IP 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5605

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、北京天融信网络安全技术有限公司、恒安嘉新(北京)科技股份公司、华为技术有限公司、深信服科技股份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、长春嘉诚信息技术股份有限公司、山东道普测评技术有限公司、北京华云安信息技术有限公司、北京云科安信科技有限公司、河南灵创电子科技有限公司、内蒙古洞明科技有限公司、

山东云天安全技术有限公司、南京众智维信息科技有限公司、泽鹿安全、远江盛邦（北京）网络安全科技股份有限公司、北京禹宏信安科技有限公司、上海观安信息技术股份有限公司、吉林谛听信息技术有限公司、北京天地和兴科技有限公司、广西网信信息技术有限公司、河南信安世纪科技有限公司、山东云天安全大数据技术有限公司、四川哨兵信息科技有限公司、信联科技（南京）有限公司、安徽长泰信息安全服务有限公司、北京智游网安科技有限公司、京东云安全及其他个人白帽子向 CNVD 提交了 4971 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 3358 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
斗象科技（漏洞盒子）	1941	1941
奇安信网神（补天平台）	1024	1024
上海交大	393	393
哈尔滨安天科技集团股份有限公司	269	0
北京天融信网络安全技术有限公司	195	22
恒安嘉新(北京)科技股份公司	119	0
华为技术有限公司	115	0
深信服科技股份有限公司	89	0
新华三技术有限公司	74	0
北京神州绿盟科技有限公司	69	2
北京启明星辰信息安全技术有限公司	65	0
北京数字观星科技有限公司	20	0
杭州安恒信息技术股份有限公司	7	7
北京知道创宇信息技术股份有限公司	5	0
国瑞数码零点实验室	117	117
长春嘉诚信息技术股份有	104	104

限公司		
山东道普测评技术有限公司	83	83
北京华云安信息技术有限公司	82	82
北京云科安信科技有限公司	80	80
河南灵创电子科技有限公司	27	27
内蒙古洞明科技有限公司	15	15
山东云天安全技术有限公司	12	12
南京众智维信息科技有限公司	11	11
泽鹿安全	11	11
远江盛邦（北京）网络安全科技股份有限公司	8	8
北京禹宏信安科技有限公司	5	5
上海观安信息技术股份有限公司	5	5
吉林谛听信息技术有限公司	5	5
北京天地和兴科技有限公司	3	3
广西网信信息技术有限公司	2	2
河南信安世纪科技有限公司	2	2
山东云天安全大数据技术有限公司	1	1
四川哨兵信息科技有限公司	1	1
信联科技（南京）有限公司	1	1
安徽长泰信息安全服务有限公司	1	1
北京智游网安科技有限公司	1	1
京东云安全	1	1

CNCERT 天津分中心	15	15
CNCERT 贵州分中心	1	1
个人	988	988
报送总计	5967	4971

本周漏洞按类型和厂商统计

本周，CNVD 收录了 252 个漏洞。应用程序 154 个，操作系统 43 个，WEB 应用 23 个，网络设备（交换机、路由器等网络端设备）16 个，安全产品 7 个，智能设备（物联网终端设备）5 个，数据库 4 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	154
操作系统	43
WEB 应用	23
网络设备（交换机、路由器等网络端设备）	16
安全产品	7
智能设备（物联网终端设备）	5
数据库	4

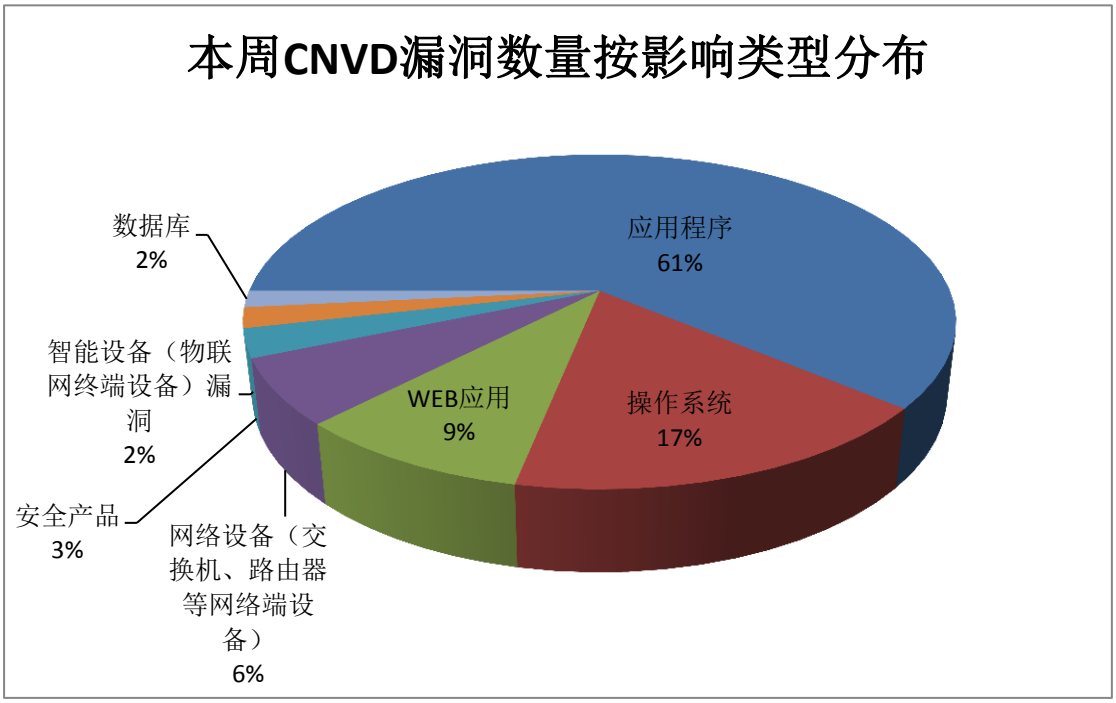

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、ZyXEL、Oracle 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	Google	38	15%
2	ZyXEL	17	6%
3	Oracle	15	6%
4	Huawei	14	6%
5	LibVNCServer	14	6%
6	F5	12	5%
7	Adobe	12	5%
8	Cisco	11	4%
9	IBM	10	4%
10	其他	109	43%

本周行业漏洞收录情况

本周，CNVD 收录了 8 个电信行业漏洞，33 个移动互联网行业漏洞，8 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-2020-36260）、Google Android System 组件缓冲区溢出漏洞（CNVD-2020-36708）、WAGO Industrial Managed Switches 852-303、852-1305 和 852-1505 信任管理问题漏洞 （CNVD-2020-36950）、Honeywell equIP 系列、Performance 系列 IP 摄像头和 Recorders 认证绕过漏洞”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/

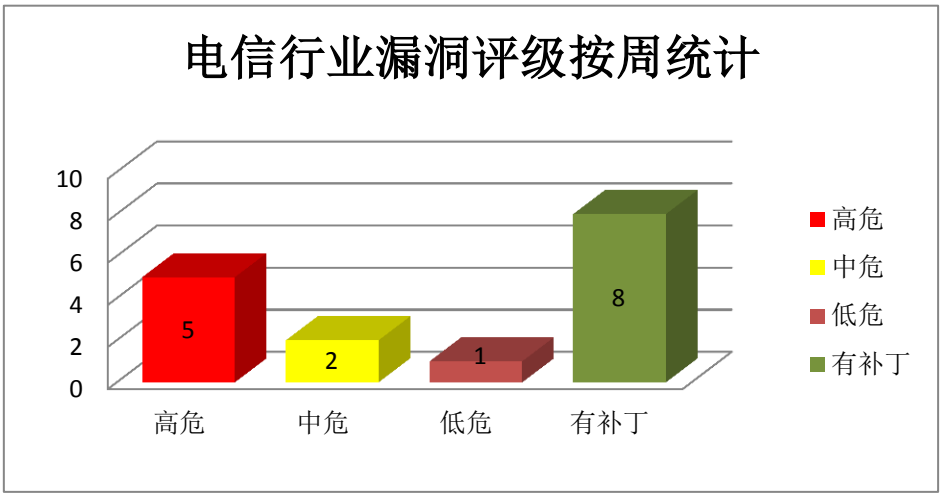

图 3 电信行业漏洞统计

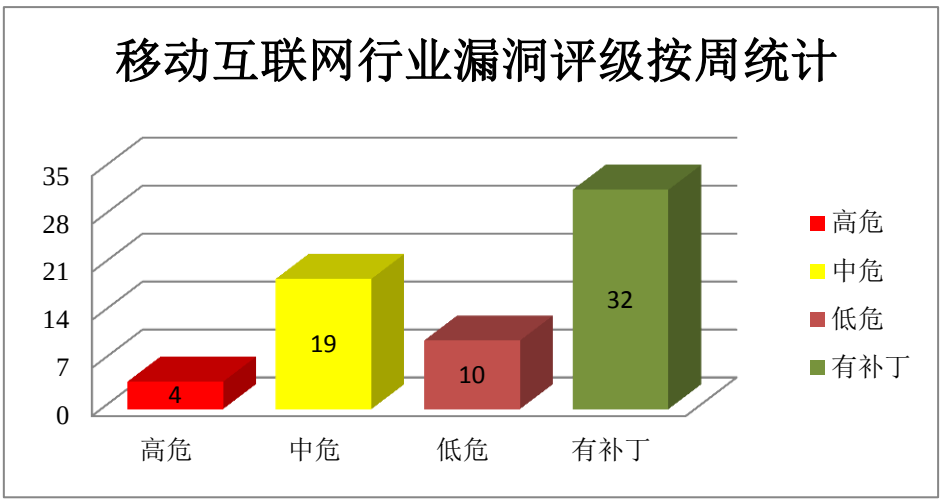

图 4 移动互联网行业漏洞统计

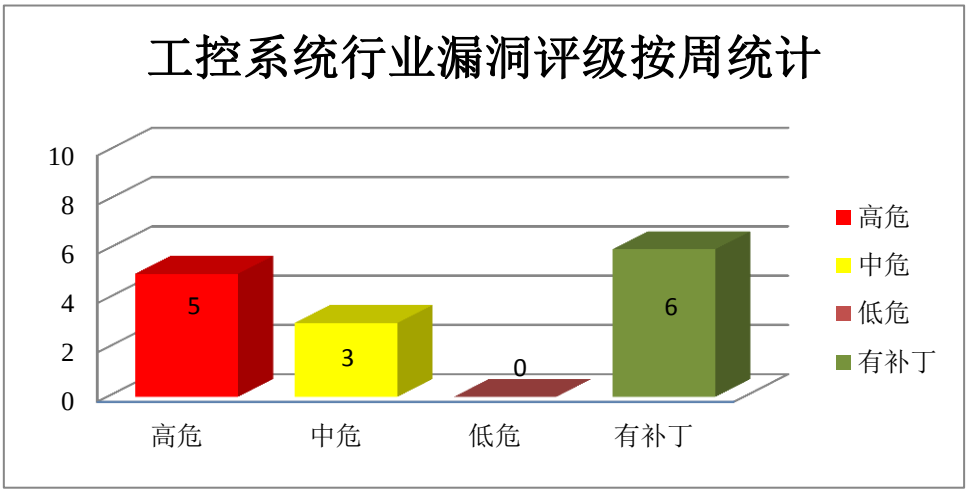

图 5 工控系统行业漏洞统计

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 Small Business RV016 Multi-WAN VPN 等都是美国思科（Cisco）公司的一款 VPN 路由器。Cisco Digital Network Architecture Center（DNA Center）是一套数字网络体系结构解决方案。Cisco Unified Contact Center Express（Unified CCX）是一款统一通信解决方案中的客户关系管理组件。Cisco AMP for Endpoints Mac Connector Software 是一套基于 macOS 平台的集成了静态和动态恶意软件分析以及威胁情报的终端应用程序。Cisco Identity Services Engine（ISE）是一款基于身份的环境感知平台（ISE 身份服务引擎）。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审核日志并获取凭据，执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-36259、CNVD-2020-36258、CNVD-2020-36257、CNVD-2020-36260）、Cisco Digital Network Architecture Center 日志信息泄露漏洞、Cisco Unified Contact Center Express 授权问题漏洞、Cisco AMP for Endpoints Mac Connector Software 拒绝服务漏洞、Cisco Identity Services Engine 拒绝服务漏洞（CNVD-2020-36263）。其中，“多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-36259、CNVD-2020-36258、CNVD-2020-36257、CNVD-2020-36260）”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-2020-36259

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36258

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36257

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36262

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36261

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36260

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36264

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36263

2、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）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多个漏洞，攻击者可利用漏洞以提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android System 组件权限提升漏洞（CNVD-2020-36706、CNVD-2020-36705、CNVD-2020-36704、CNVD-2020-36707）、Google Android System 组件缓冲区溢出漏洞（CNVD-2020-36709、CNVD-2020-36708）、Google Android System 组件资源管理错误漏洞（CNVD-2020-36710）、Android Media Framework 权限提升漏洞（CNVD-2020-36750）。其中，“Google Android System 组件缓冲区溢

出漏洞（CNVD-2020-36708）、Google Android System 组件资源管理错误漏洞（CNVD-2020-36710）、Android Media Framework 权限提升漏洞（CNVD-2020-36750）”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-2020-36706

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36705

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36704

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36709

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36708

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36707

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36710

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36750

3、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。Secospace USG6600 是一款下一代防火墙产品。CloudEngine 6800 是一款面对数据中心的 6800 系列万兆以太网交换机。CloudEngine 12800 是一款 12800 系列数据中心交换机。Huawei Honor View 20 等都是一款智能手机。USG6600 是一款数据中防火墙产品。OSCA-550AX 是一款 55 寸智慧屏。OSCA-550A 是一款 55 寸采用华为鸿蒙操作系统的终端智慧屏。CloudUSM 是华为企业云通信解决方案的核心交换设备，为语音、视频、移动应用、多媒体会议等业务提供统一的会话和媒体控制平台。AP2000 是一款无线接入点设备。IPS Module 是一款入侵防御系统（IPS）模块。NGFW Module 是一款下一代防火墙（NGFW）模块。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，执行非法操作，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei NIP6800、Secospace USG6600 和 USG9500 内存泄露漏洞（CNVD-2020-36723）、Huawei CloudEngine 6800 和 Huawei CloudEngine 12800 拒绝服务漏洞、Huawei Honor 20 PRO、Honor View 20 和 Honor 20 处理不当漏洞、Huawei NIP6800、Secospace USG6600 和 USG9500 IPSec 模块重复释放内存漏洞、多款 Huawei 产品验证不足漏洞、Huawei CloudUSM-EUA 信息泄露漏洞、Huawei NIP6800、Secospace USG6600 和 USG9500 IPSec 模块越界读漏洞、多款 Huawei 产品越界读取漏洞（CNVD-2020-36735）。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-2020-36723

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36725

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36724

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36730

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36729

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36732

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36731

https://www.cnvd.org.cn/flaw/show/CNVD-2020-36735

4、Adobe 产品安全漏洞

Adobe DNG Software Development Kit（SDK）是美国奥多比（Adobe）公司的一款提供读取和写入 DNG 文件功能的软件开发工具包。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe DNG Software Development Kit 缓冲区溢出漏洞（CNVD-2020-38188、CNVD-2020-38187、CNVD-2020-38186、CNVD-2020-38191、CNVD-2020-38190、CNVD-2020-38189、CNVD-2020-38193、CNVD-2020-38192）。其中，“Adobe DNG Software Development Kit 缓冲区溢出漏洞（CNVD-2020-38191、CNVD-2020-38190、CNVD-2020-38193、CNVD-2020-38192）”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-2020-38188

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38187

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38186

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38191

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38190

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38189

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38193

https://www.cnvd.org.cn/flaw/show/CNVD-2020-38192

5、Honeywell ControlEdge PLC 和 ControlEdge RTU 信息泄露漏洞

Honeywell ControlEdge PLC 和 ControlEdge RTU 都是美国霍尼韦尔（Honeywell）公司的产品。ControlEdge PLC 是一款可编程逻辑控制器（PLC）。ControlEdge RTU 是一款远程终端单元（RTU）。本周，Honeywell ControlEdge PLC 和 RTU 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取未加密的密码。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-2020-37480

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	修复方式

		评级	
CNVD-2020-36383	F5 BIG-IP 远程代码执行漏洞	高	目前，F5 官方已发布新版本修复此漏洞，CNVD 建议用户立即升级至最新版本：https://support.f5.com/csp/article/K52145254
CNVD-2020-36384	IBM DB2 缓冲区溢出漏洞（CNVD-2020-36384）	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.ibm.com/support/pages/node/6242332
CNVD-2020-36521	Linux kernel 输入验证错误漏洞（CNVD-2020-36521）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b86dab054059b970111b5516ae548efaae5b3aae
CNVD-2020-36790	LibVNCServer 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：https://github.com/LibVNC/libvncserver/commit/74e8a70f2c9a5248d6718ce443e07c7ed314dfff
CNVD-2020-36941	WordPress Drag and Drop Multi File Upload - Contact Form 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://www.codedropz.com/
CNVD-2020-36949	多款 Emerson Electric 产品访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.emerson.com/
CNVD-2020-36951	WAGO 750-88x Series 和 WAGO 750-87x Series 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://www.wago.com/de/download/public/Sicherheitshinweis-SA-SYS-2019-001/SA-SYS-2019-001.pdf
CNVD-2020-37832	Microsoft Windows Now Playing Session Manager 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1201
CNVD-2020-37938	Linux kernel 缓冲区溢出漏洞（CNVD-2020-37938）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.6.7
CNVD-2020-37946	Qualcomm SM8150 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://www.qualcomm.com/company/product-security/bulletins/june-2020-security-bulletin

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞访问审核日志并获取凭据，执行任意代码，导致拒绝服务。此外，Google、Huawei、Adobe 等多款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。另外，Honeywell ControlEdge PLC 和 RTU 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取未加密的密码。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、ZyXEL Armor X1 WAP6806 路径遍历漏洞

验证描述

ZyXEL Armor X1 WAP6806 是中国台湾合勤（ZyXEL）公司的一款无线网卡产品。

ZyXEL Armor X1 WAP6806 1.00(ABAL.6)C0 版本中存在路径遍历漏洞。该漏洞源于网络系统或产品未能正确地过滤资源或文件路径中的特殊元素。攻击者可利用该漏洞访问受限目录之外的位置。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2020060088

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-36768

信息提供者

恒安嘉新(北京)科技股份公司

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. Zoom 修复了影响 Windows 7 的零日 RCE 错误，即将推出更多更新

Zoom 网络会议客户端包含一个零日漏洞，该漏洞可能使攻击者能够在易受攻击的系统上远程执行命令。

参考链接：https://www.bleepingcomputer.com/news/security/zoom-fixes-zero-day-rce-bug-affecting-windows-7-more-updates-soon/

2. Citrix 发布了 11 个新的安全缺陷补丁

Citrix 昨天发布了针对多个产品的 11 个安全缺陷的补丁，这些缺陷影响了其 Citrix 应用交付控制器（ADC），网关和 SD-WAN WAN 优化版（WANOP）网络产品。

参考链接：https://thehackernews.com/2020/07/citrix-software-security-update.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