国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 07 月 01 日-2019 年 07 月 07 日 **2019 年第 27 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 207 个，其中高危漏洞 74 个、中危漏洞 103 个、低危漏洞 30 个。漏洞平均分值为 6.03。本周收录的漏洞中，涉及 0day 漏洞 103 个（占 50%），其中互联网上出现“D-Link DIR-823G 命令注入漏洞（CNVD-2019-20996）、SuperMicro SuperDoctor 任意代码执行漏洞”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 3343 个，与上周（2575 个）环比增长 30%。

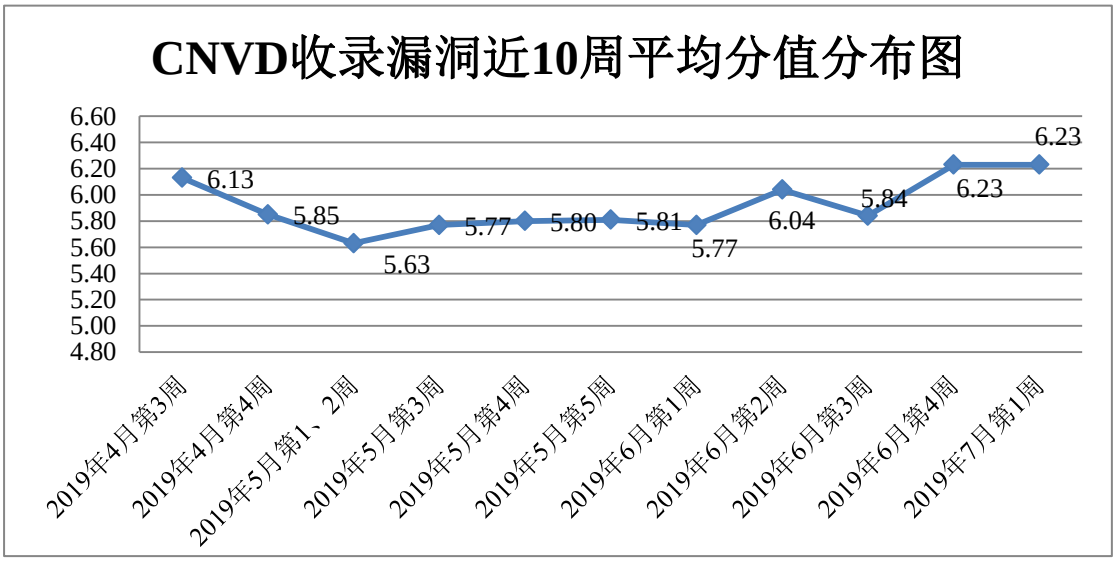

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 5 起，向银行、保险、能源等重要行业单位通报漏洞事件 20 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 263 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 85 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15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：

北京京东世纪贸易有限公司、灵宝简好网络科技有限公司、厦门才茂通信科技有限公司、郑州路之易科技有限公司、北京致远互联软件股份有限公司、长沙米拓信息技术有限公司、浙江齐治科技股份有限公司、淄博闪灵网络科技有限公司、山西牛酷信息科技有限公司、上海步科自动化股份有限公司、深圳市卓越迈创企业形象设计有限公司、深圳市英之杰网络科技有限公司、上海馨煜信息科技有限公司、中铁十九局集团有限公司、中国建筑一局（集团）有限公司、台湾永宏电机股份有限公司、天津市网城天创科技有限责任公司、广州中爆安全网科技有限公司、云南天罡北斗信息科技有限公司、中电网(北京)电子科技发展有限公司、北京蓝海迅捷通信技术有限公司、杭州希和信息技术有限公司、河南中钰网络科技公司、蓝信网络科技有限公司、安徽华易网络科技有限公司、北京夜猫网络科技有限公司、南京医健通信息科技有限公司、上海卓卓网络科技有限公司、中国中铁四局集团有限公司、中铁十二局集团第四工程有限公司、中国中铁一局集团第四工程有限公司、沧州市凡诺广告传媒有限公司、北京标软信息技术有限公司、中铁十八局集团第五工程有限公司、成都依能科技股份有限公司、桂林崇胜网络科技有限公司、网易公司、海洋 CMS、DocCms X 开发团队、亿渡留言管理系统、苹果CMS、EasyAdmin 极简社区、梦想 CMS、YzmCMS、FastAdmin、CatfishCMS、HDCMS、SaxueCMS、PHPEMS、KUNBUS 和 zzzcms。

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、新华三技术有限公司、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。长春嘉诚信息技术股份有限公司、国网思极检测技术（北京）有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、南京众智维信息科技有限公司、任子行网络技术股份有限公司、山石网科通信技术有限公司、重庆贝特计算机系统工程有限公司、北京圣博润高新技术股份有限公司、山东华鲁科技发展股份有限公司、杭州安信检测技术有限公司、河南信安世纪科技有限公司、广州锦行网络科技有限公司、上海并擎软件科技有限公司、新疆海狼科技有限公司、北京智游网安科技有限公司、北京信联科汇科技有限公司、福建省海峡信息技术有限公司、郑州赛欧思科技有限公司及其他个人白帽子向 CNVD 提交了 3343 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1891 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）	1447	1447
奇安信网神（补天平台）	444	444
北京天融信网络安全技术有限公司	275	4
哈尔滨安天科技集团股份有限公司	211	0
华为技术有限公司	162	0
新华三技术有限公司	78	0
深信服科技股份有限公司	67	0
恒安嘉新(北京)科技股份公司	47	1
北京神州绿盟科技有限公司	40	2
厦门服云信息科技有限公司	22	0
北京数字观星科技有限公司	10	0
北京知道创宇信息技术股份有限公司	2	0
四川无声信息技术有限公司	36	36
中新网络信息安全股份有限公司	23	23
南京联成科技发展股份有限公司	10	
长春嘉诚信息技术股份有限公司	113	113
国网思极检测技术（北京）有限公司	107	107
国瑞数码零点实验室	824	824
内蒙古奥创科技有限公司	36	36
南京众智维信息科技有限公司	30	30
任子行网络技术股份有限公司	25	25

山石网科通信技术有限公司	14	14
重庆贝特计算机系统工程有限公司	9	9
北京圣博润高新技术股份有限公司	7	7
山东华鲁科技发展股份有限公司	7	7
杭州安信检测技术有限公司	6	6
河南信安世纪科技有限公司	5	5
广州锦行网络科技有限公司	2	2
上海并擎软件科技有限公司	2	2
新疆海狼科技有限公司	2	2
北京智游网安科技有限公司	1	1
北京信联科汇科技有限公司	1	1
福建省海峡信息技术有限公司	1	1
郑州赛欧思科技有限公司	1	1
CNCERT 天津分中心	20	20
CNCERT 四川分中心	5	5
CNCERT 贵州分中心	2	2
CNCERT 西藏分中心	2	2
个人	164	164
报送总计	4260	3343

本周漏洞按类型和厂商统计

本周，CNVD 收录了 207 个漏洞。应用程序 113 个，WEB 应用 51 个，网络设备（交换机、路由器等网络端设备）22 个，操作系统 10 个，安全产品 6 个，智能设备（物联网终端设备）漏洞　5 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	113
WEB 应用	51
网络设备（交换机、路由器等网络端设备）	22
操作系统	10
安全产品	6
智能设备（物联网终端设备）漏洞	5

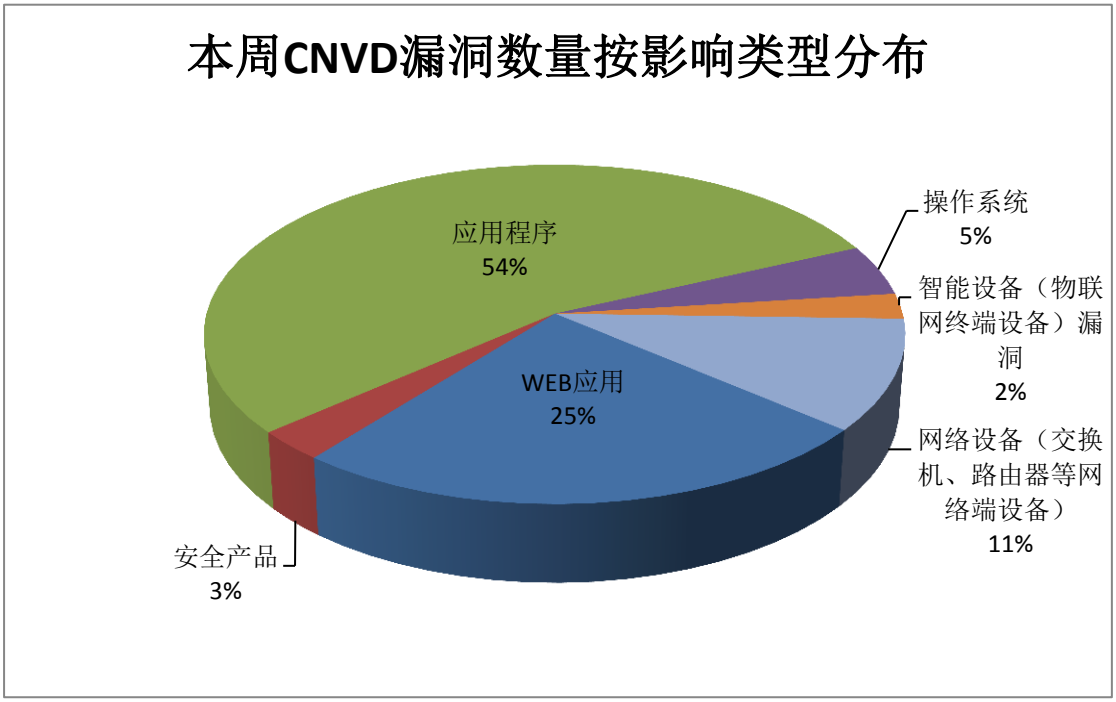

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Google、Cisco 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	IBM	20	10%
2	Google	11	5%
3	Cisco	9	4%
4	PHP Scripts Mall	8	4%
5	Synology	8	4%
6	Adobe	6	3%
7	D-Link	6	3%
8	LiveZilla	5	2%

9	McAfee	5	2%
10	其他	129	63%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，7 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，“Cisco Unified Communications Manager 缓冲区溢出漏洞（CNVD-2019-21308）、Google Android System 组件远程代码执行漏洞（CNVD-2019-21310）、BD Alaris Gateway Workstation 任意文件上传漏洞”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，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/

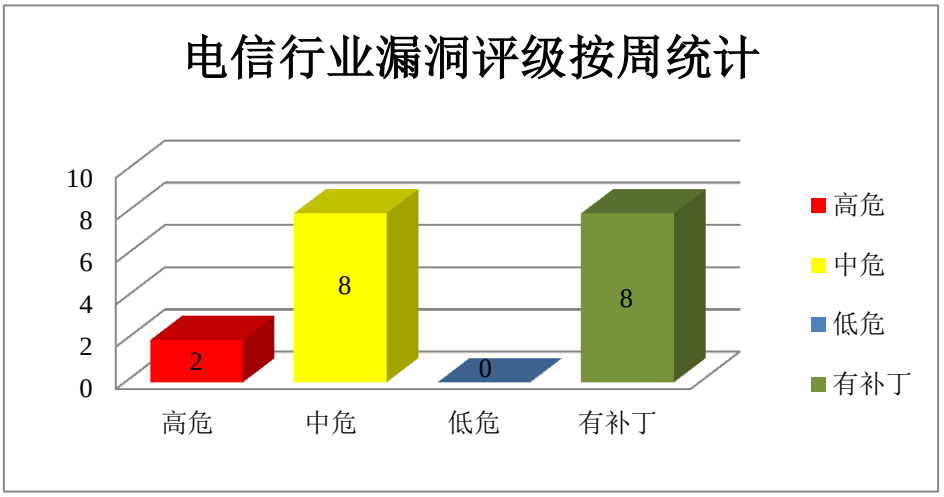

图 3 电信行业漏洞统计

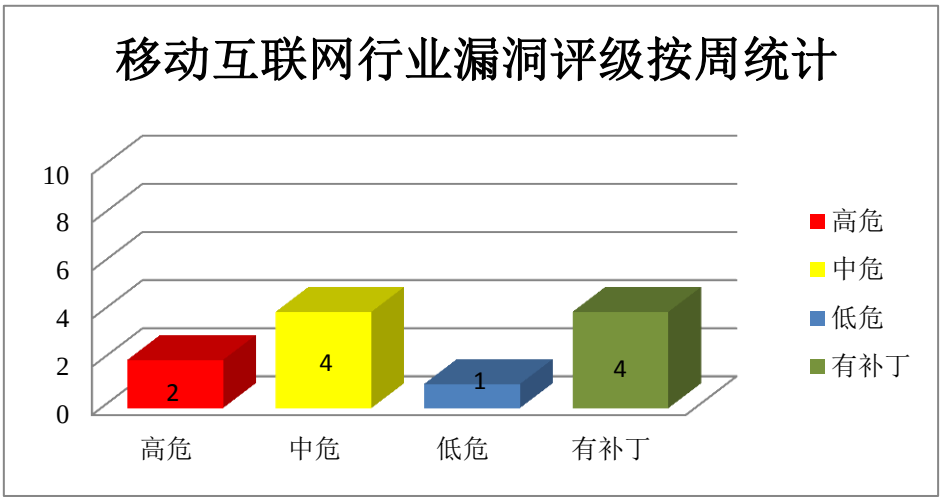

图 4 移动互联网行业漏洞统计

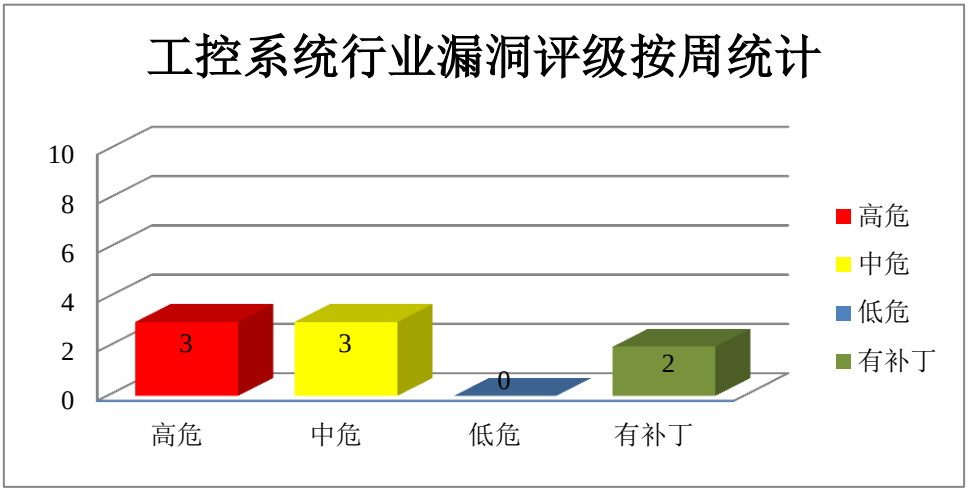

图 5 工控系统行业漏洞统计

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 Rational Collaborative Lifecycle Management（CLM）是一套协作化生命周期管理解决方案。IBM Planning Analytics 是一套业务规划分析解决方案。IBM Robotic Process Automation with Automation Anywhere 是一套流程自动化解决方案。IBM Spectrum Protect（前称 Tivoli Storage Manager）是一套数据保护平台。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，执行未授权操作，执行任意代码或造成服务器或 Storage Agents 崩溃等。

CNVD 收录的相关漏洞包括：IBM Rational Quality Manager 跨站脚本漏洞（CNVD-2019-20855）、IBM Planning Analytics 跨站脚本漏洞（CNVD-2019-20988）、IBM Robotic Process Automation with Automation Anywhere 信息泄露漏洞（CNVD-2019-20991、CNVD-2019-20993、CNVD-2019-20994）、IBM Robotic Process Automation with Automation Anywhere LDAP 注入漏洞、IBM Spectrum Protect 缓冲区溢出漏洞、IBM Spectrum Protect Operations Center 信息泄露漏洞。其中，“IBM Spectrum Protect 缓冲区溢出漏洞”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-2019-20855

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20988

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20991

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20993

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20994

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20995

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21078

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21258

2、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。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，该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，绕过安全限制并执行未授权的操作，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2019-21124）、Google Android System 组件信息泄露漏洞（CNVD-2019-21262、CNVD-2019-21261、CNVD-2019-21263、CNVD-2019-21264）、Google Android System 组件权限提升漏洞（CNVD-2019-21266、CNVD-2019-21265）、Google Android System 组件远程代码执行漏洞（CNVD-2019-21310）。其中，“Google Android System 组件权限提升漏洞（CNVD-2019-21266、CNVD-2019-21265）、Google Android System 组件远程代码执行漏洞（CNVD-2019-21310）”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-2019-21124

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21262

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21261

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21263

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21266

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21265

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21264

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21310

3、Cisco 产品安全漏洞

Cisco Advanced Malware Protection（AMP）for Endpoints for Windows 是一款基于 Windows 平台的端点安全解决方案。Cisco Firepower Management Center（FMC）是新一代防火墙管理中心软件。Cisco Email Security Appliance（ESA）是一个电子邮件安全设备。AsyncOS Software 是运行在其中的一套操作系统。Cisco IOS XR 是一套为其网络设备开发的操作系统。Cisco Web Security Appliance（WSA）是一款 Web 安全设备。Cisco Unified Communications Manager（CUCM，Unified CM，CallManager）是一款统一通信系统中的呼叫处理组件。Cisco Nexus 9000 Series Fabric Switches 是一款 9000 系列光纤交换机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Advanced Malware Protection for Endpoints for Windows 命令注入漏洞、Cisco Firepower Management Center 跨站脚本漏洞（CNV

D-2019-21297、CNVD-2019-21303）、Cisco Email Security Appliance 输入验证错误漏洞、Cisco IOS XR 输入验证错误漏洞、Cisco Web Security Appliance AsyncOS Software 输入验证错误漏洞、Cisco Unified Communications Manager 缓冲区溢出漏洞（CNVD-2019-21308）、Cisco Nexus 9000 Series Fabric Switches 访问控制错误漏洞。其中，“Cisco Advanced Malware Protection for Endpoints for Windows 命令注入漏洞、Cisco Unified Communications Manager 缓冲区溢出漏洞（CNVD-2019-21308）”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-2019-21275

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21297

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21303

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21304

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21306

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21307

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21308

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21309

4、Synology 产品安全漏洞

Synology Photo Station 是一套用于在互联网上共享图片、视频和博客的解决方案。Synology Calendar 是一款运行在 Synology NAS（网络存储服务器）设备上的文件保护程序。Synology Office 是一套基于 Web 的办公软件系统。Synology Moments 是一款图像和视频分类管理应用程序。Synology Note Station 是一款基于云的笔记管理应用程序。Synology Calendar 是一款运行在 Synology NAS（网络存储服务器）设备上的文件保护程序。Synology Universal Search 是一款用于搜索 Synology NAS 中的应用程序和文件的软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞执行非法 SQL 命令或进行跨站攻击等。

CNVD 收录的相关漏洞包括：Synology Photo Station SQL 注入漏洞（CNVD-2017-27712）、Synology Photo Station 路径遍历漏洞、Synology Calendar 跨站脚本漏洞（CNVD-2019-20976）、Synology Office 跨站脚本漏洞（CNVD-2019-20978）、Synology Moments 路径遍历漏洞、Synology Note Station 跨站脚本漏洞（CNVD-2019-20979）、Synology Calendar 操作系统命令注入漏洞、Synology Universal Search Highlight Preview 授权漏洞。其中，“Synology Photo Station SQL 注入漏洞（CNVD-2017-27712）、Synology Calendar 操作系统命令注入漏洞、Synology Universal Search Highlight Preview 授权漏洞”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-2019-20975

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20974

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20976

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20978

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20980

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20979

http://www.cnvd.org.cn/flaw/show/CNVD-2019-20981

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21426

7、Motorola CX2L MWR04L 栈溢出漏洞

Motorola CX2L MWR04L 是一款无线路由器。Motorola CX2L MWR04L 被披露存在栈溢出漏洞。攻击者可借助 8010 TCP 端口和 8080 UDP 端口利用该漏洞造成拒绝服务（无限递归和栈消耗）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-20990

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-2019-20858	Magento 跨站请求伪造漏洞（CNVD-2019-20858）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://magento.com/security/patches/supee-11155
CNVD-2019-20977	Chamilo LMS 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://support.chamilo.org/projects/1/wiki/Security_issues
CNVD-2019-20983	CSZ CMS SQL 注入漏洞	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/cskaza/cszcms/issues/19
CNVD-2019-21066	Prima FlexAir 数据库配置备份下载漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://primasystems.eu/flexair-access-control/
CNVD-2019-21069	Prima FlexAir 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://primasystems.eu/flexair-access-control/
CNVD-2019-21113	多款 ZOHO 产品授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.com/product

			s/desktop-central/elevation-of-privilege-vulnerability.html
CNVD-2019-21114	Citrix SD-WAN Center/Appliance 多个漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.citrix.com/downloads/citrix-sd-wan/
CNVD-2019-21241	BD Alaris Gateway Workstation 任意文件上传漏洞	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.bd.com/
CNVD-2019-21251	FreeBSD 缓冲区溢出漏洞（CNVD-2019-21251）	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.freebsd.org/security/advisories/FreeBSD-SA-19:09.iconv.asc
CNVD-2019-21252	EBK BKS Buskoppler 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，详情请关注厂商主页：https://www.g-u.com/

小结：本周，IBM 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行未授权操作，执行任意代码或造成服务器或 Storage Agents 崩溃等。此外，Google、Cisco、Synology 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，绕过安全限制并执行未授权的操作，进行跨站攻击，提升权限，执行任意代码，造成拒绝服务等。Motorola CX2L MWR04L 被披露存在栈溢出漏洞。攻击者可借助 8010 TCP 端口和 8080 UDP 端口利用该漏洞造成拒绝服务（无限递归和栈消耗）。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、SuperMicro SuperDoctor 任意代码执行漏洞

验证描述

SuperMicro SuperDoctor 是美国 SuperMicro 公司的一套服务器管理监控平台。该平台主要用于实时监控目标节点硬件在数据中心的系统运行状况或可用性。

Super Micro SuperDoctor 5 版本中存在安全漏洞。远程攻击者可借助 NRPE 利用该漏洞执行任意命令。

验证信息

POC 链接：https://www.exploit-db.com/exploits/47030

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-21071

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. 研究人员发现医疗软件漏洞，将导致诊断结果有误

近期研究人员最新发现了一个用于基因组分析的通用开源软件的漏洞，这将导致基于 DNA 的医学诊断很容易受到网络攻击。桑迪亚国家实验室的研究人员发现了这个弱点，并及时通知了软件开发人员，随后他们发布了一个补丁来解决这个问题，同时最新版本的软件也解决了这个问题。虽然目前还不知道该漏洞是否遭受过攻击，但国家标准技术研究院最近在给软件开发人员、基因组学研究人员和网络管理员的一份说明中对该漏洞进行了分析。这一发现揭示了保护基因组信息不仅仅涉及个人基因信息的安全存储，而分析基因数据的计算机系统中的网络安全也是至关重要的。

参考链接：https://news.mydrivers.com/1/634/634978.htm

2. 谷歌挖出 iMessage 新漏洞，运行旧系统的 iPhone 只能重置修复

近日，谷歌 Project Zero 团队曝光了一个重大的 iMessage 漏洞。若用户收到一组特定的字符，iPhone 可能会变得一团糟。这个 bug 会导致受害者的 iPhone 被锁定，唯一的解决方案就是恢复出厂设置，意味着你将无法恢复未保存的丢失数据。在 Mac 上，这个 bug 会导致 soagent 崩溃重启。但在 iPhone 上，该代码位于 Springboard 中。即便经过了硬件重置，该问题依然存在，一旦解锁就会导致手机无法使用。若用户手上的 iPhone 运行的是 iOS 12.3 之前的版本，他们会在面对该问题时束手无策。

参考链接：https://www.cnbeta.com/articles/tech/864763.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