国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 08 月 26 日-2019 年 09 月 01 日　　2019 年第 35 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 401 个，其中高危漏洞 79 个、中危漏洞 267 个、低危漏洞 55 个。漏洞平均分值为 5.44。本周收录的漏洞中，涉及 0day 漏洞 34 个（占 8%），其中互联网上出现“ABUS Secvest FUAA50000 消息传输错误条件漏洞、Vera Edge Home Controller 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 2022 个，与上周（1865 个）环比增长 9%。

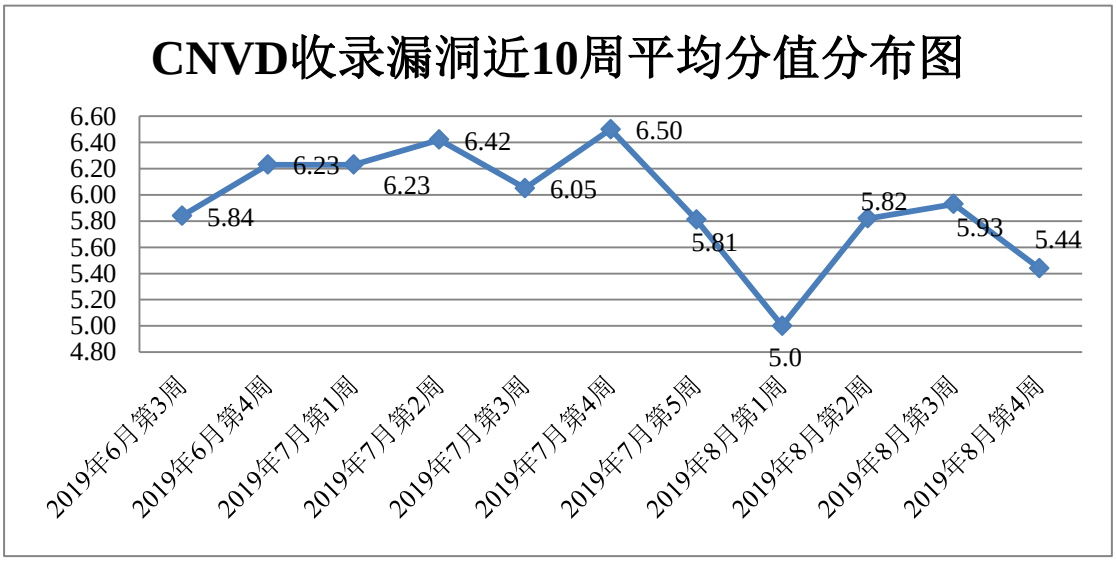

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 19 起，向银行、保险、能源等重要行业单位通报漏洞事件 26 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 644 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 86 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 18 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：

淄博闪灵网络科技有限公司、解放日报社、东莞市同享软件科技有限公司、北京正影网络科技有限公司、斑斓信息科技（上海）有限公司、浙江自贸区耀光网络科技有限公司、成都任我行科技有限公司、苏州恩斯特网络科技有限公司、中国化学工程集团有限公司、成都鹏博士电信传媒集团股份有限公司、北京超越无限信息技术有限公司、ShopXO、南昌蓝智科技有限公司、洪湖尔创网联信息技术有限公司、zzzcms、上海卓卓网络科技有限公司、国药堂大药房(上海)有限公司、广东盈世计算机科技有限公司、中国城镇化促进会、中铁大桥局集团有限公司、山西先启科技有限公司、SemCms、北京城建六建设集团有限公司、四川挚梦科技有限公司、深圳市哈烁实业有限公司、中国建筑第八工程局有限公司、UQCMS、MyBB Group、中国电机工程学会、朋友圈网络科技有限公司、长沙友点软件科技有限公司、北京通达信科科技有限公司、杭州联创信息技术有限公司、中国工控 ABB 中国客户服务中心、广州市保伦电子有限公司、上海汉得信息技术股份有限公司、中国新闻传媒网、中国展览馆协会、正方软件股份有限公司、扬州市青锐网络科技有限公司和杭州钜警佰源信息技术有限公司。

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、北京神州绿盟科技有限公司、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、山东云天安全技术有限公司、北京铭图天成信息技术有限公司、国瑞数码零点实验室、任子行网络技术股份有限公司、山东新潮信息技术有限公司、北京圣博润高新技术股份有限公司、广州锦行网络科技有限公司、内蒙古奥创科技有限公司、北京君信安科技有限公司、贵州安码科技有限公司、山东华鲁科技发展股份有限公司、北京智游网安科技有限公司、河南信安世纪科技有限公司、山石网科通信技术有限公司、上海市信息安全测评认证中心及其他个人白帽子向 CNVD 提交了 2022 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 1584 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）	954	954

斗象科技（漏洞盒子）	630	630
哈尔滨安天科技集团股份有限公司	410	0
北京天融信网络安全技术有限公司	218	5
北京神州绿盟科技有限公司	106	1
华为技术有限公司	99	0
深信服科技股份有限公司	72	0
新华三技术有限公司	58	0
恒安嘉新(北京)科技股份公司	57	0
北京启明星辰信息安全技术有限公司	41	0
厦门服云信息科技有限公司	35	0
西安四叶草信息技术有限公司	27	27
北京数字观星科技有限公司	19	0
北京知道创宇信息技术股份有限公司	7	4
远江盛邦（北京）网络安全科技股份有限公司	51	51
山东云天安全技术有限公司	34	34
北京铭图天成信息技术有限公司	33	33
国瑞数码零点实验室	30	30
任子行网络技术股份有限公司	25	25
山东新潮信息技术有限公司	16	16
北京圣博润高新技术股份有限公司	11	11
广州锦行网络科技有限公司	11	11
内蒙古奥创科技有限公司	6	6

北京君信安科技有限公司	6	6
贵州安码科技有限公司	4	4
山东华鲁科技发展股份有限公司	4	4
北京智游网安科技有限公司	2	2
河南信安世纪科技有限公司	1	1
山石网科通信技术有限公司	1	1
上海市信息安全测评认证中心	1	1
CNCERT 山西分中心	12	12
CNCERT 甘肃分中心	11	11
CNCERT 湖南分中心	9	9
CNCERT 贵州分中心	6	6
CNCERT 河北分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 北京分中心	1	1
CNCERT 西藏分中心	1	1
个人	121	121
报送总计	3134	2022

本周漏洞按类型和厂商统计

本周，CNVD 收录了 401 个漏洞。应用程序 284 个，WEB 应用 42 个，操作系统 40 个，网络设备（交换机、路由器等网络端设备）13 个，安全产品 11 个，数据库 6 个，智能设备（物联网终端设备）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	284
WEB 应用	42

操作系统	40
网络设备（交换机、路由器等网络端设备）	13
安全产品	11
数据库	6
智能设备（物联网终端设备）	5

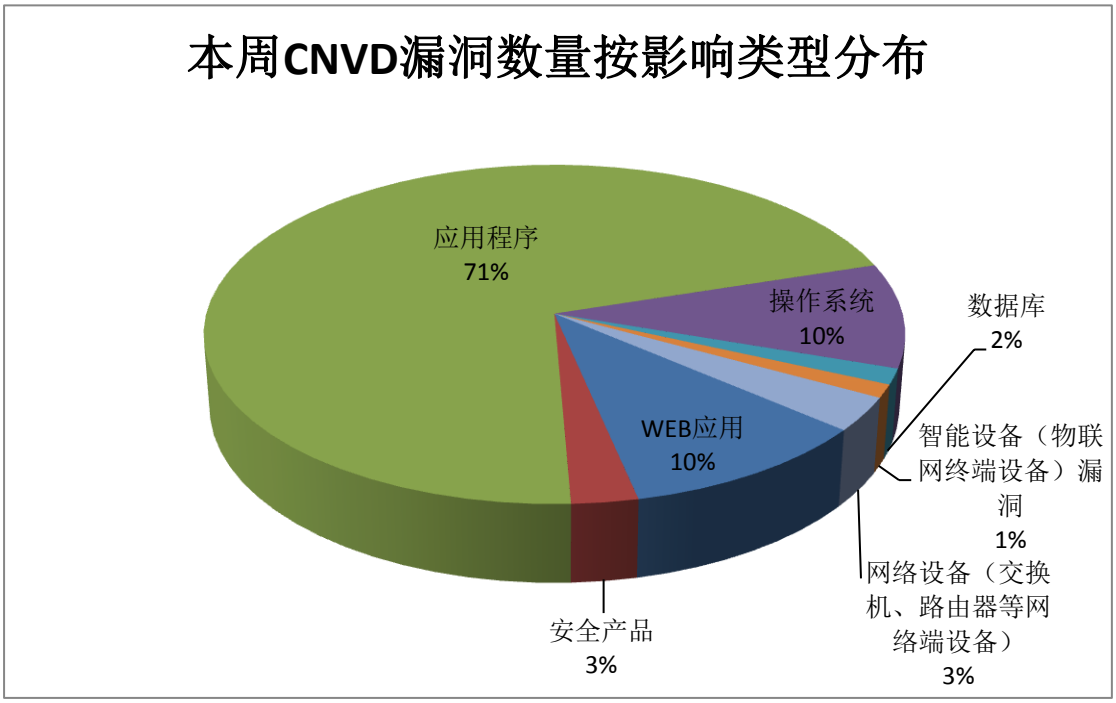

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 cPanel、WordPress、Adobe 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	cPanel	73	18%
2	WordPress	38	10%
3	Adobe	37	10%
4	Oracle	29	7%
5	ImageMagick Studio	25	6%
6	Linux	15	4%
7	Google	14	3%
8	IBM	13	3%
9	Cisco	12	3%
10	其他	145	36%

本周行业漏洞收录情况

本周，CNVD 收录了 1 个电信行业漏洞，14 个移动互联网行业漏洞（如下图所示）。其中，“Alfresco Software Alfresco application for Android SQL 注入漏洞”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/

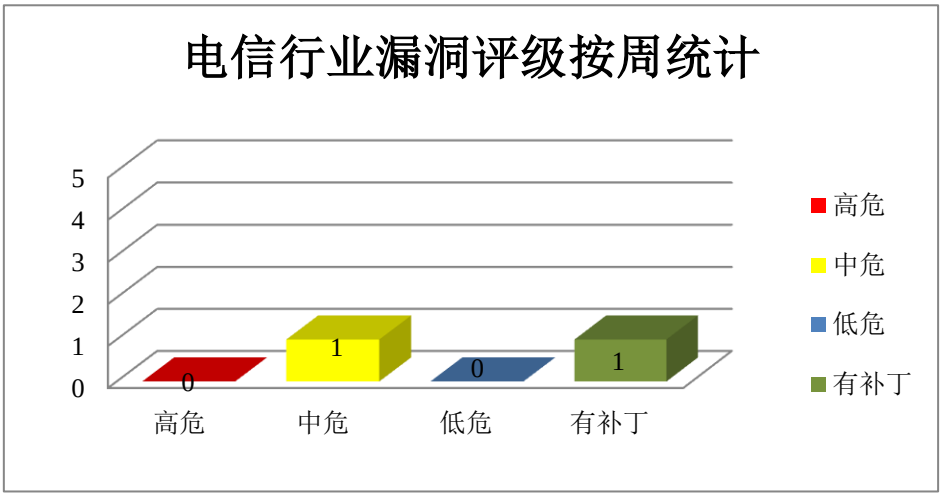

图 3 电信行业漏洞统计

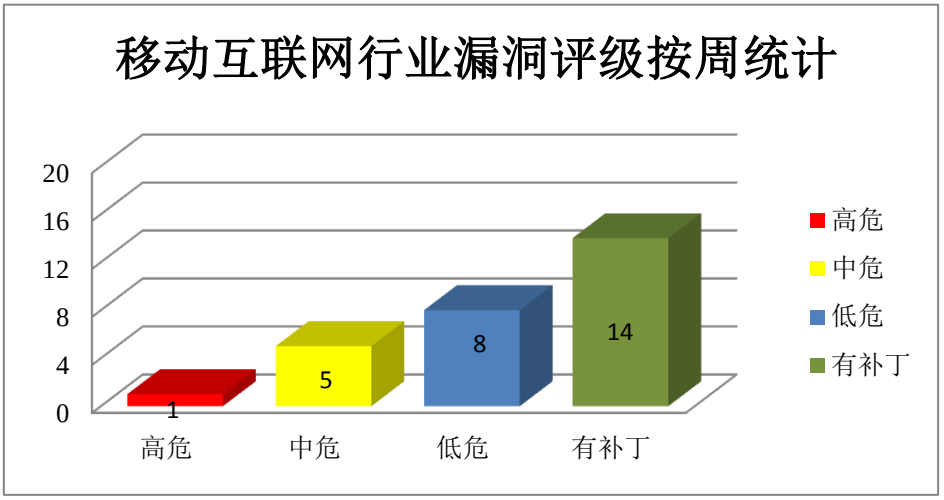

图 4 移动互联网行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在越界读取和越界写入漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 越界读取漏洞、Adobe Acrobat/Reader 越界写入漏洞（CNVD-2019-29553、CNVD-2019-29554、CNVD-2019-29555、CNVD-2019-29559、CNVD-2019-29557、CNVD-2019-29560、CNVD-2019-29561）。其中，除“Adobe Acrobat/Reader 越界读取漏洞、Adobe Acrobat/Reader 越界写入漏洞（CNVD-2019-29553）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-28879
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29553
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29554
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29555
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29559
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29557
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29560
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29561

2、Oracle 产品安全漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。Oracle E-Business Suite（电子商务套件）是一套全面集成式的全球业务管理软件。本周，该产品被披露存在访问控制错误漏洞，攻击者可利用漏洞攻击者可利用该漏洞未授权读取、更新、插入或删除数据，影响数据的保密性和完整性。

CNVD 收录的相关漏洞包括：Oracle BI Publisher 访问控制错误漏洞（CNVD-2019-29186、CNVD-2019-29191、CNVD-2019-29192）、Oracle BI Publisher 组件访问控制错误漏洞（CNVD-2019-29188）、Oracle Marketing 组件访问控制错误漏洞（CNVD-2019-29193、CNVD-2019-29194、CNVD-2019-29195、CNVD-2019-29196）。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-2019-28879
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29186
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29188
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29191
http://www.cnvd.org.cn/flaw/show/CNVD-2019-29193

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29194

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29195

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29192

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29196

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29553

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。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拒绝服务，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2019-29107）、Linux kernel 代码问题漏洞、Linux kernel 缓冲区溢出漏洞（CNVD-2019-29563、CNVD-2019-29637、CNVD-2019-29638、CNVD-2019-29641、CNVD-2019-29639、CNVD-2019-29640）。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-2019-29107

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29563

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29596

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29637

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29638

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29641

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29639

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29640

4、IBM 产品安全漏洞

IBM Informix Dynamic Server（IDS）是一款可扩展的对象关系数据库服务器，它为集群数据中心提供持续数据可用性和灾难恢复等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取管理员权限。

CNVD 收录的相关漏洞包括：IBM Informix Dynamic Server 缓冲区溢出漏洞（CNVD-2019-29421、CNVD-2019-29422）、IBM Informix Dynamic Server 权限许可和访问控制问题漏洞（CNVD-2019-29420、CNVD-2019-29423、CNVD-2019-29424、CNVD-2019-29425、CNVD-2019-29427、CNVD-2019-29426）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-29420

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29421

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29422

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29423

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29424

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29425

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29427

http://www.cnvd.org.cn/flaw/show/CNVD-2019-29426

6、Lenovo Solution Center 提权漏洞

Lenovo Solution Center（LSC）是一套用于帮助用户快速识别系统健康状态、网络连接和整个系统安全状态的软件。本周，Lenovo Solution Center 被披露存在提权漏洞，攻击者可利用该漏洞提升权限。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-2019-28704

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-2019-28882	WordPress olimometer 插件 SQL 注入漏洞（CNVD-2019-28882）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wordpress.org/plugins/olimometer/#developers
CNVD-2019-29131	Facebook HHVM 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://hhvm.com/blog/2019/06/10/hhvm-4.9.0.html
CNVD-2019-29134	GNU patch 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://git.savannah.gnu.org/cgit/patch.git/commit/?id=3fcd042d26d70856e826a42b5f93dc4854d80bf0
CNVD-2019-29138	Synetics i-doit 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.i-doit.com/
CNVD-2019-29143	Google Chrome Blink 资源管理错误漏洞（CNVD-2019-29143）	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/2019/08/stable-channel-update-for-desktop_26.html?m=1
CNVD-2019-29148	Apache Subversion svnserve servers 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://subversion.apache.org/security/CVE-2019-0203-advisory.txt
CNVD-201	Cisco IOS XE Software 授权	高	厂商已发布了漏洞修复程序，请及时

9-29411	问题漏洞		关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass
CNVD-2019-29441	BEdita 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/bedita/bedita/pull/1608
CNVD-2019-29447	Spoon Library 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/forkcms/library/pull/69
CNVD-2019-29605	cPanel 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://documentation.cpanel.net/display/CL/68+Change+Log

小结：本周，Adobe 被披露存在越界读取和越界写入漏洞，攻击者可利用漏洞执行任意代码。此外，Oracle、Linux、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取管理员权限，造成拒绝服务，导致缓冲区溢出或堆溢出等。另外，Lenovo Solution Center 被披露存在提权漏洞，攻击者可利用该漏洞提升权限。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、ABUS Secvest FUAA50000 消息传输错误条件漏洞

验证描述

ABUS Secvest FUAA50000 是德国 ABUS 公司的一款无线遥控器。

ABUS Secvest FUAA50000 存在安全漏洞。攻击者可利用漏洞抑制正确接收未经授权的无线报警系统，例如状态探测器发出的指示入侵的信息。

验证信息

POC 链接：https://packetstormsecurity.com/files/153780/ABUS-Secvest-3.01.01-Unchecked-Message-Transmission-Error-Condition.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-29126

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. Hickory 智能门锁存在的多个漏洞

近期，某安全研究团队发现了 Hickory 蓝牙智能系列 BlueTooth Enabled Deadbolt 款式门锁存在多个安全漏洞，漏洞涉及其移动端 APP 应用和云托管的 Web 服务和 MQTT 协议。截至漏洞披露期限前，Hickory 官方还未对这些漏洞作出认可，也未发布任何补丁或漏洞修复措施。

参考链接：https://www.freebuf.com/vuls/211095.html

2. 新的物联网僵尸网络正在感染基于 Android 的机顶盒

一个名为 Ares 的新 IoT 僵尸网络正在感染基于 Android 的设备， 网络安全公司 WootCloud 表示，受影响最多的是由 HiSilicon，Cubetek 和 QezyMedia 制造的 Android 机顶盒。这些攻击并未使用 Android 操作系统中的漏洞，而是利用在机顶盒安装中已启用且未受保护的配置服务。

参考链接：https://www.zdnet.com/article/a-new-iot-botnet-is-infecting-android-based-set-top-boxes/

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