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 08 日-2019 年 07 月 14 日 **2019 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 316 个，其中高危漏洞 123 个、中危漏洞 170 个、低危漏洞 23 个。漏洞平均分值为 6.42。本周收录的漏洞中，涉及 0day 漏洞 157 个（占 50%），其中互联网上出现“WordPress CRUDLab WP Like Button 插件身份验证漏洞、D-Link DIR-818LW 命令注入漏洞（CNVD-2019-22213）”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 2528 个，与上周（3353 个）环比下降 25%。

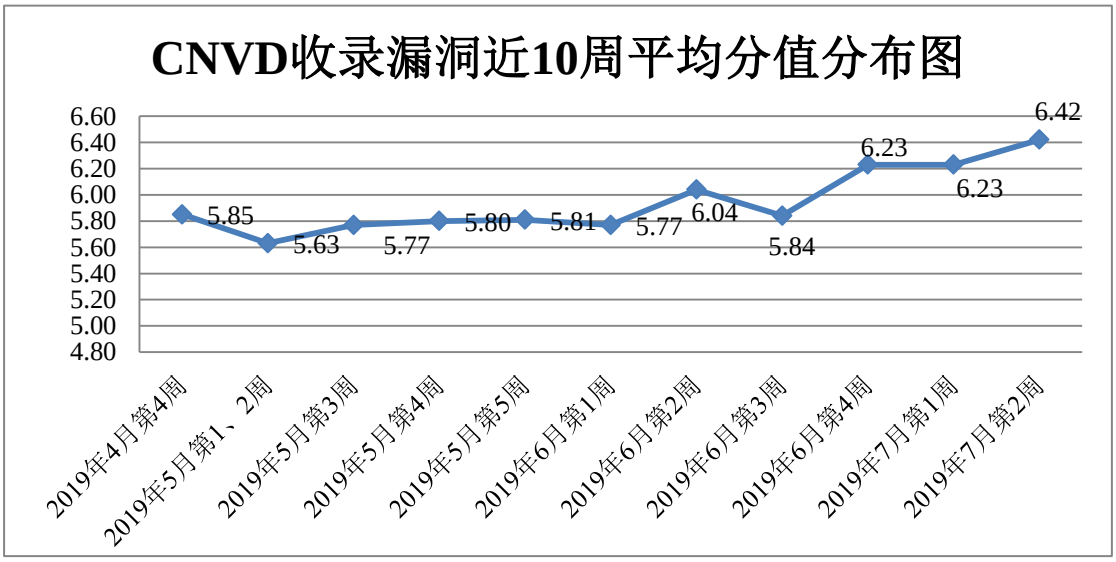

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 2 起，向银行、保险、能源等重要行业单位通报漏洞事件 29 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 335 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 43 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16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：

锐捷网络股份有限公司、华拓信息技术有限公司、欧姆龙自动化（中国）有限公司、桂林崇胜网络科技有限公司、张家界玉米科技有限公司、北京亿源通科技有限公司、甘肃成兴信息科技有限公司、广州齐博网络科技有限公司、苏州托普斯网络科技有限公司、北京超越无限信息技术有限公司、上海小蚁科技有限公司、山大鲁能信息科技有限公司、上海卓卓网络科技有限公司、苏州烟火网络科技有限公司、深圳市吉祥腾达科技有限公司、智士软件（北京）有限公司、佛山市顺德区出格软件设计有限公司、海南赞赞网络科技有限公司、上海泛微软件有限公司、四川天府星空网络科技有限公司、研华科技（中国）有限公司、永康跨海网络有限公司、北京通达信科科技有限公司、北京心海导航教育科技股份有限公司、全讯汇聚网络科技（北京）有限公司、友讯电子设备（上海）有限公司、杭州迪普科技股份有限公司、北京米尔伟业科技有限公司、广州搜客网络科技有限公司、互诺科技、中国互联网新闻中心、海洋 CMS、zzzcms、HUSTOJ、DOYOCMS、CatfishCMS 和 ZZCMS。

本周，CNVD 发布了《关于 Redis 存在远程命令执行漏洞的安全公告》和《Microsoft 发布 2019 年 7 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5115

https://www.cnvd.org.cn/webinfo/show/5117

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、深信服科技股份有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。内蒙古奥创科技有限公司、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、广州锦行网络科技有限公司、长春嘉诚信息技术股份有限公司、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、北京铭图天成信息技术有限公司、杭州安信检测技术有限公司、山石网科通信技术有限公司、成都云娱中天网络科技有限公司、河南信安世纪科技有限公司、福建省海峡信息技术有限公司、江苏安又恒信息科技有限公司、浙江鹏信信息科技股份有限公司及其他个人白帽子向 CNVD 提交了 2528 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 1781 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）	1339	1339
奇安信网神（补天平台）	442	442
北京天融信网络安全技术有限公司	434	5
哈尔滨安天科技集团股份有限公司	230	0
华为技术有限公司	114	0
深信服科技股份有限公司	113	0
新华三技术有限公司	56	0
北京神州绿盟科技有限公司	41	0
恒安嘉新(北京)科技股份公司	30	1
中新网络信息安全股份有限公司	23	23
厦门服云信息科技有限公司	18	2
北京数字观星科技有限公司	10	0
四川无声信息技术有限公司	8	8
百度安全响应中心（BSRC）	5	5
北京知道创宇信息技术股份有限公司	4	4
北京启明星辰信息安全技术有限公司	3	3
国瑞数码零点实验室	200	200
国网思极检测技术（北京）有限公司	150	150
内蒙古奥创科技有限公司	34	34
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	19	19
广州锦行网络科技有限公司	16	16

长春嘉诚信息技术股份有限公司	10	10
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	5	5
北京铭图天成信息技术有限公司	4	4
杭州安信检测技术有限公司	3	3
山石网科通信技术有限公司	3	3
成都云娱中天网络科技有限公司	2	2
河南信安世纪科技有限公司	2	2
福建省海峡信息技术有限公司	1	1
江苏安又恒信息科技有限公司	1	1
浙江鹏信信息科技股份有限公司	1	1
CNCERT 西藏分中心	12	12
CNCERT 天津分中心	9	9
CNCERT 黑龙江分中心	5	5
CNCERT 贵州分中心	2	2
CNCERT 海南分中心	2	2
CNCERT 宁夏分中心	1	1
个人	182	182
报送总计	3566	2528

本周漏洞按类型和厂商统计

本周，CNVD 收录了 316 个漏洞。应用程序 172 个，WEB 应用 89 个，操作系统 26 个，网络设备（交换机、路由器等网络端设备）23 个，安全产品 2 个，数据库 2 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	172
WEB 应用	89
操作系统	26
网络设备（交换机、路由器等网络端设备）	23
安全产品	2
数据库	2
智能设备（物联网终端设备）	2

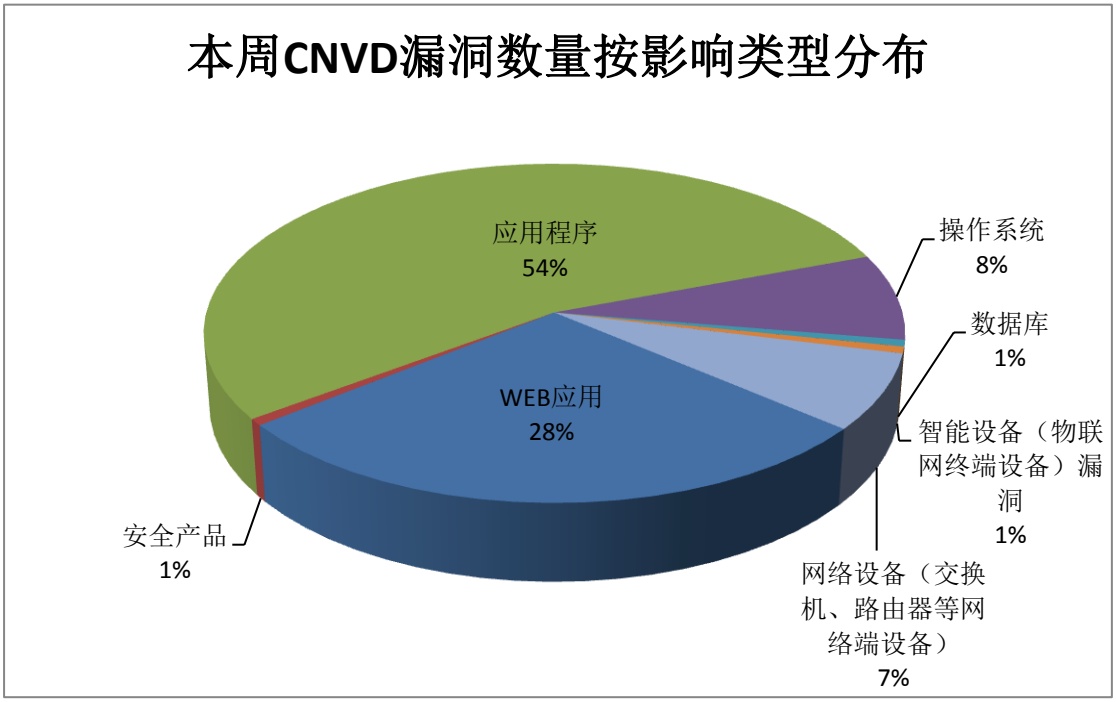

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Foo Labs、GNU 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	Adobe	28	9%
2	Foo Labs	22	7%
3	GNU	21	7%
4	WordPress	18	6%
5	Foxit	16	5%
6	Apple	15	5%
7	Microsoft	14	4%

8	Xnview	13	4%
9	ImageMagick Studio	10	3%
10	其他	159	50%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，13 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“EdgeMAX EdgeSwitch 命令注入漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-21981）、Siemens TIA Administrator 身份验证漏洞、Apple tvOS 和 Apple iOS GeoServices 内存破坏漏洞”等漏洞的综合评级为“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/

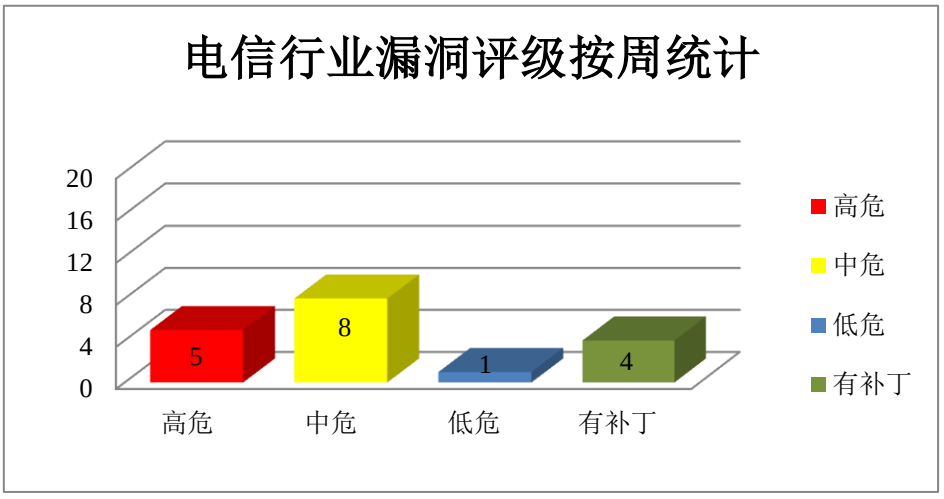

图 3 电信行业漏洞统计

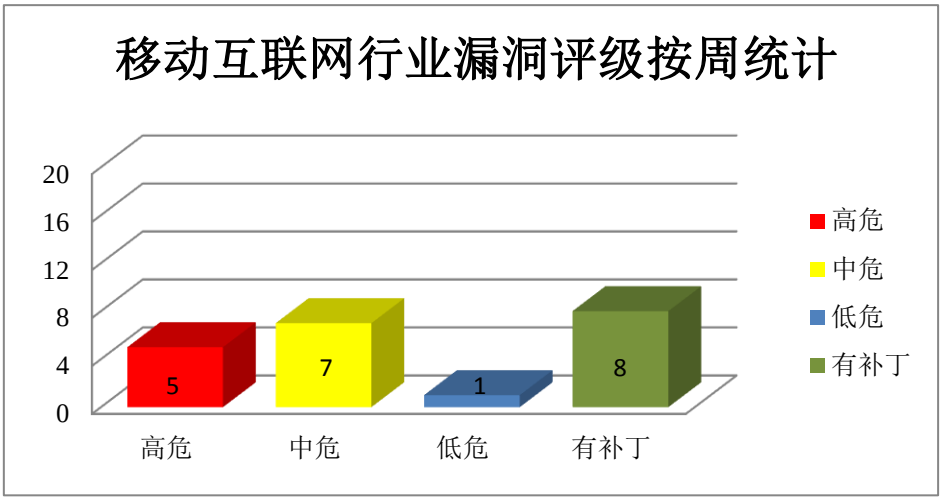

图 4 移动互联网行业漏洞统计

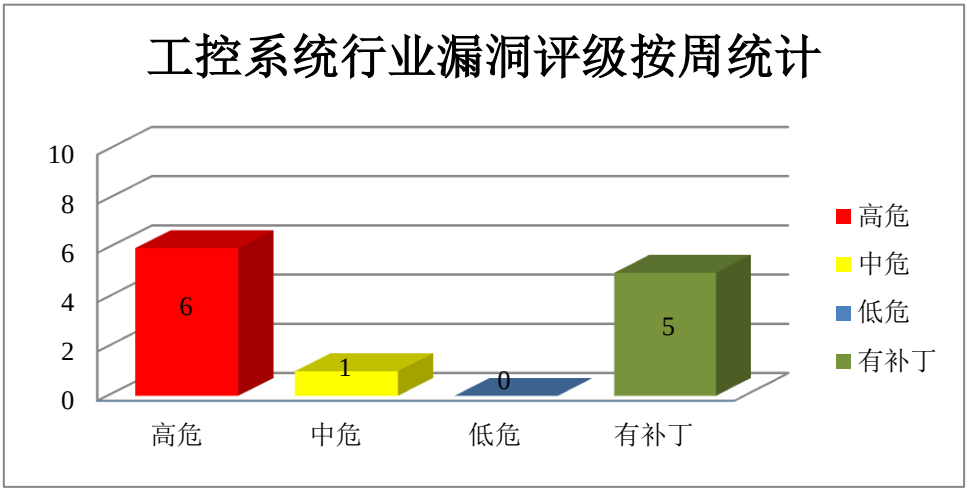

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft .NET Framework 是一种全面且一致的编程模型，也是一个用于构建 Windows、Windows Store、Windows Phone、Windows Server 和 Microsoft Azure 的应用程序的开发平台。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 Exchange Server 是一套电子邮件服务程序。本周，上述产品被披露存在提权和拒绝服务漏洞，攻击者可利用漏洞提升权限，执行任意代码或造成拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft .NET Framework 拒绝服务漏洞（CNVD-2019-22203）、Microsoft Windows 提权漏洞（CNVD-2019-22215、CNVD-2019-22217、CNVD-2019-22218）、Microsoft Windows Audio Service 提权漏洞、Microsoft Windows Kernel 提权漏洞（CNVD-2019-22219、CNVD-2019-22222）、Microsoft win32k 提权漏洞。其中，除“Microsoft .NET Framework 拒绝服务漏洞（CNVD-2019-22203）、Microsoft Windows 提权漏洞（CNVD-2019-22217、CNVD-2019-22218）”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-2019-22203

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22215

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22214

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22217

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22219

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22218

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22220

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22222

2、Foxit 产品安全漏洞

Foxit PDF SDK ActiveX 是一个 PDF 软件开发工具包，也是一个可视化编程组件。Foxit PhantomPDF 是一款多功能 PDF 编辑器。Foxit Reader 是一款 PDF 文档阅读器。本周，该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。

CNVD 收录的相关漏洞包括：Foxit PDF SDK ActiveX 资源管理错误漏洞（CNVD-2019-21956）、Foxit Reader AcroForm 内存错误引用漏洞、Foxit PhantomPDF Calculate 内存错误引用漏洞、Foxit Reader Text removeField 远程代码执行漏洞漏洞、Foxit Reader AcroForm exportValues 远程代码执行漏洞、Foxit PhantomPDF addWatermarkFromText 远程代码执行漏洞、Foxit PhantomPDF Button Calculate 远程代码执行漏洞、Foxit Reader XFA Form 远程代码执行漏洞。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-2019-21956

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22460

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22461

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22462

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22464

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22465

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22466

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22467

3、Apple 产品安全漏洞

Apple iCloud for Windows 是一款基于 Windows 平台的云服务，它支持存储音乐、照片、App 和联系人等。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple Safari 是一款 Web 浏览器，是 MacOSX 和 iOS 操作系统附带的默认浏览器。Apple iOS 是为移动设备所开发的一套操作系统。Apple tvOS 是一套智能电视操作系统。WebKit 是其中的一个 Web 浏览器引擎组件。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，获取提升的权限，执行任意代码，造成应用程序意外终止（内存破坏）。

CNVD 收录的相关漏洞包括：Apple iCloud for Windows 竞争条件漏洞、Apple macOS Mojave Security 内存错误引用漏洞、Apple macOS Mojave QuartzCore 内存破坏漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-21981）、多款 Apple 产品 WebKit 类型混淆漏洞（CNVD-2019-21983）、Apple iOS Safari 未授权访问漏洞、Apple tvOS 和 Apple iOS GeoServices 内存破坏漏洞、Apple iOS、tvOS 和 macOS Mojave Ker

nel 逻辑漏洞。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-2019-21974

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21975

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21978

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21981

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21983

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21984

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21987

http://www.cnvd.org.cn/flaw/show/CNVD-2019-21988

4、Adobe 产品安全漏洞

Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。Adobe Acrobat 是一款 PDF 编辑软件。本周，该产品被披露存在越界写入漏洞，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 越界写入漏洞（CNVD-2019-22469、CNVD-2019-22468、CNVD-2019-22470、CNVD-2019-22471、CNVD-2019-22472、CNVD-2019-22473、CNVD-2019-22474、CNVD-2019-22475）。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-2019-22469

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22468

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22470

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22471

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22472

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22473

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22474

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22475

5、Redis 未授权访问漏洞（CNVD-2019-21763）

Redis 是一个开源的使用 ANSI C 语言编写，支持网络，可基于内存亦可持久化的日志型，Key-Value 数据库，并提供多种语言的 API。Redis 被披露存在未授权访问漏洞。攻击者可利用该漏洞在未授权访问 Redis 的情况下执行任意代码，获取目标服务器权限。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-2019-21763

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-2019-21653	Adobe Flash Player 内存错误引用漏洞（CNVD-2019-21653）	高	厂商已发布漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/flash-player/apsb19-26.html
CNVD-2019-21754	Zoom Client DOS 漏洞	高	用户可联系供应商获得补丁信息：https://medium.com/@jonathan.leitschuh/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5
CNVD-2019-21935	JetBrains IntelliJ IDEA 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://blog.jetbrains.com/blog/2019/06/19/jetbrains-security-bulletin-q1-2019/
CNVD-2019-22204	Intel Processor Diagnostic Tool 权限提升漏洞（CNVD-2019-22204）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://downloadcenter.intel.com/download/19792/Intel-Processor-Diagnostic-Tool
CNVD-2019-22212	EdgeMAX EdgeSwitch 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://community.ui.com/releases/EdgeMAX-EdgeSwitch-Firmware-v1-8-2/824d58b1-6027-49cf-878d-2076c01948b7
CNVD-2019-22240	Siemens SIPROTEC 5 和 Siemens DIGISI 5 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://cert-portal.siemens.com/productcert/pdf/ssa-899560.pdf
CNVD-2019-22386	WordPress Rencontre 插件 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://wordpress.org/plugins/rencontre/#developers
CNVD-2019-22477	Adobe Acrobat/Reader 越界写入漏洞（CNVD-2019-22477）	高	厂商已发布漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb19-07.html
CNVD-2019-22235	Siemens TIA Administrator 身份验证漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/pdf/ssa-721298.pdf
CNVD-2019-22393	WordPress WP Live Chat Support Pro 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://wordpress.org/plugins/wp-live-chat-support/#developers

小结：本周，Microsoft 被披露存在提权和拒绝服务漏洞，攻击者可利用漏洞提升权限，执行任意代码或造成拒绝服务。此外，Foxit、Apple、Adobe 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访问，获取提升的权限，执行任意代码，造成应用程序意外终止（内存破坏）。Redis 被披露存在未授权访问漏洞。攻击者可利用该漏洞在未授权访问 Redis 的情况下执行任意代码，获取目标服务器权限。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、WordPress CRUDLab WP Like Button 插件身份验证漏洞

验证描述

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。CRUDLab WP Like Button plugin 是使用在其中的一个用于在页面上添加按钮的插件。

WordPress CRUDLab WP Like Button 插件 1.6.0 及之前版本中存在插件身份验证绕过漏洞。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进行未经身份验证更改插件的设置。

验证信息

POC 链接：https://www.exploit-db.com/exploits/47078

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-22385

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. GE 麻醉机中发现的漏洞

医院中使用的某些麻醉机固件中的漏洞可能会被滥用，以改变正常功能，直至调整吸入物质的混合水平。该漏洞影响 GE Aestiva 和 GE Aespire 麻醉系统，型号 7100 和 7900，来自 GE Healthcare。研究人员建议不要将易受攻击的麻醉机连接到医院网络。

参考链接：https://www.bleepingcomputer.com/news/security/bug-in-anesthesia-machin

es-allows-changing-gas-mix-levels/

2. K12.com 暴露了多达 700 万条涉及学生个人信息的数据库记录

在线教育平台 K12.com 本周无意中暴露了近 700 万学生的个人信息。暴露的数据库包含全名，电子邮件地址，出生日期和性别身份，以及学生就读的学校，同时还可访问其帐户的身份验证密钥和其他内部数据。这些信息在线提供了一个多星期，目前还不清楚数据库是否被恶意行为者访问或者获取。据发现数据暴露的研究人员称，该问题影响了 K12.com 的 A+nyWhere 学习系统（A + LS），该系统被美国 1100 多个学区使用。

参考链接：https://www.cnbeta.com/articles/tech/867469.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