国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 01 月 28 日-2019 年 02 月 10 日 **2019 年第5、6 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 205 个，其中高危漏洞 51 个、中危漏洞 134 个、低危漏洞 20 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 68 个（占 33%），其中互联网上出现“Microsoft Windows .CONTACT File / HTML Injection Mailto:远程代码执行漏洞、Allen-Bradley PowerMonitor 1000 跨站脚本漏洞”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 1761 个，与上周（1638 个）环比增长 8%。

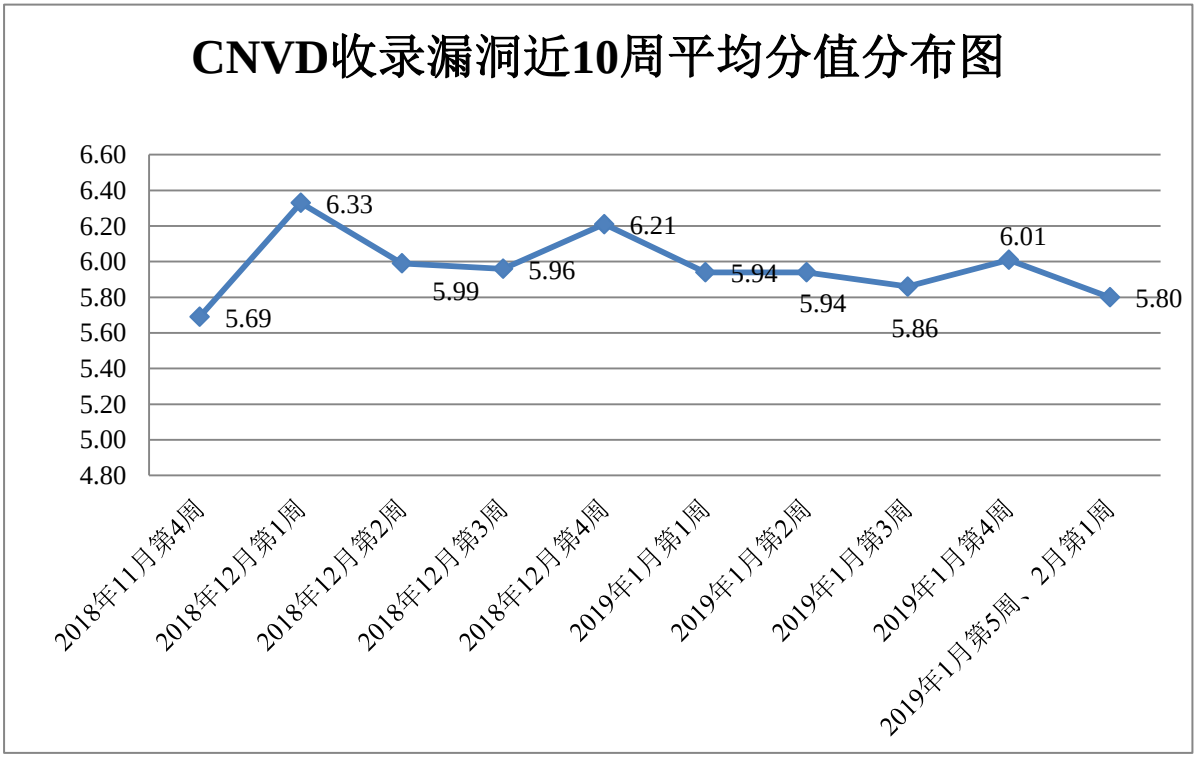

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向银行、保险、能源等重要行业单位通报漏洞事件 79 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 613 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 365 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 41 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：

上海诺基亚贝尔股份有限公司、武汉舜通智能科技有限公司、长沙米拓信息技术有限公司、北京夜猫网络科技有限公司、CIZION 股份有限公司、北京世纪超星信息技术发展有限责任公司、青岛商至信网络科技有限公司、上海丹帆网络科技有限公司、广州市顺天计算机科技有限公司、苏州托普斯网络科技有限公司、合肥首嘉网络科技有限公司、青岛聚城网络科技有限公司、南充市老虎云网络技术有限公司、南京同企信息科技有限公司、厦门易商网络科技有限公司、江苏汇学信息技术有限公司、用友网络科技股份有限公司、中控科技集团有限公司、安平县金信桥网络科技有限公司、北京易维云数据科技有限公司、四川思途智旅软件有限公司、海南创想未来文化传媒有限公司、洪湖尔创网联信息技术有限公司、重庆扬浪科技有限责任公司、成都康菲顿特网络科技有限公司、深圳市华德安科技有限公司、山西牛酷信息科技有限公司、北京东华原医疗设备有限责任公司、米酷资源网、树洞外链、162100 网站、爱特 CMS、海洋 CMS、大米 CMS、Shop7z 和 HDCMS。

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、华为技术有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。天津市国瑞数码安全系统股份有限公司、山东云天安全技术有限公司、中新网络信息安全股份有限公司、任子行网络技术股份有限公司、安徽锋刃信息科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京圣博润高新技术股份有限公司、上海观安信息技术股份有限公司、山石网科通信技术股份有限公司、北京长亭科技有限公司、江苏博智软件科技股份有限公司、广州万方计算机科技有限公司、山东华鲁科技发展股份有限公司、四川博全科技有限公司及其他个人白帽子向 CNVD 提交了 1761 个以事件型漏洞为主的原创漏洞，其中包括 360 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 1120 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）	681	681
360 网神（补天平台）	439	439
哈尔滨安天科技集团股份有限公司	166	0
华为技术有限公司	119	0
新华三技术有限公司	99	0
北京启明星辰信息安全技术有限公司	85	2
北京天融信网络安全技术有限公司	78	5
中国电信集团系统集成有限责任公司	24	0
北京神州绿盟科技有限公司	23	0
恒安嘉新(北京)科技股份公司	14	0
厦门服云信息科技有限公司	7	0
北京知道创宇信息技术有限公司	4	0
天津市国瑞数码安全系统股份有限公司	232	232
山东云天安全技术有限公司	40	40
中新网络信息安全股份有限公司	31	31
任子行网络技术股份有限公司	26	26
安徽锋刃信息科技有限公司	14	14
远江盛邦（北京）网络安全科技股份有限公司	10	10
北京圣博润高新技术股份有限公司	8	8
上海观安信息技术股份有限公司	8	8
山石网科通信技术股份有限公司	4	4

北京长亭科技有限公司	2	2
江苏博智软件科技股份有限公司	1	1
广州万方计算机科技有限公司	1	1
山东华鲁科技发展股份有限公司	1	1
四川博全科技有限公司	1	1
CNCERT 贵州分中心	3	3
CNCERT 四川分中心	2	2
CNCERT 浙江分中心	1	1
个人	249	249
报送总计	2373	1761

本周漏洞按类型和厂商统计

本周，CNVD 收录了 205 个漏洞。应用程序漏洞 126 个，操作系统漏洞 31 个，WEB 应用漏洞 30 个，网络设备漏洞 16 个，数据库漏洞 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
应用程序漏洞	126
操作系统漏洞	31
WEB 应用漏洞	30
网络设备漏洞	16
数据库漏洞	2

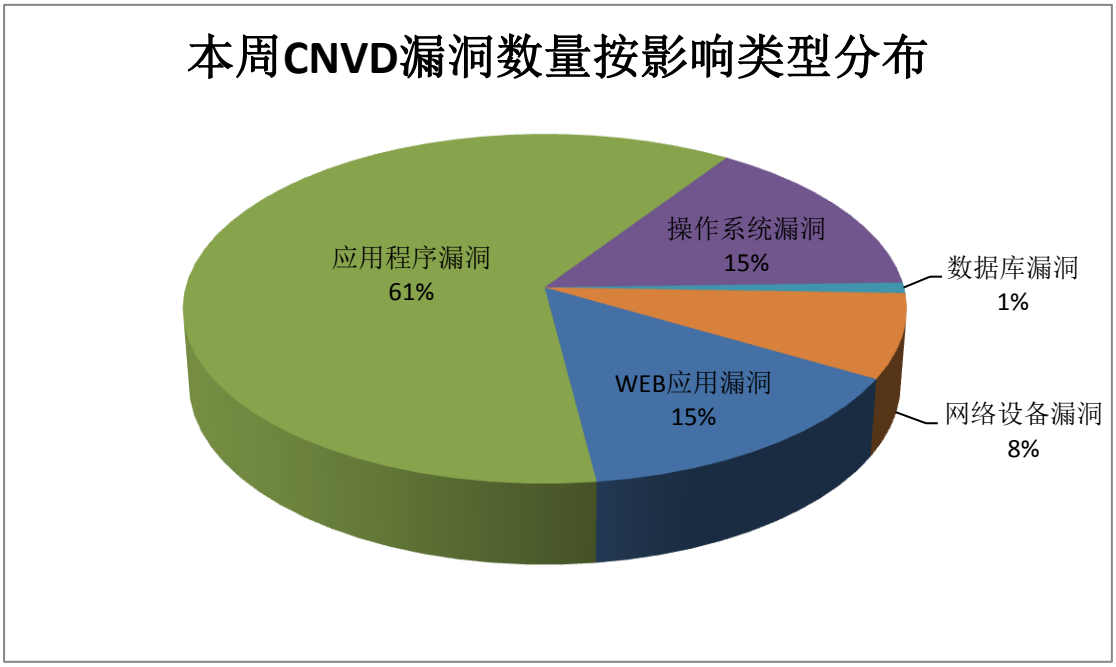

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Apple、HDF5 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	48	24%
2	Apple	19	10%
3	HDF5	15	7%
4	HPE	11	5%
5	Battelle Memorial Institute	8	4%
6	Monstra CMS	8	4%
7	Fuji Electric	7	3%
8	Schneider Electric	7	3%
9	Synology	6	3%
10	其他	76	37%

本周行业漏洞收录情况

本周，CNVD 收录了 3 个电信行业漏洞，30 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Phoenix Contact FL SWITCH 拒绝服务漏洞、Apple iOS 和 macOS Mojave WebRTC 内存破坏漏洞、WUZHI CMS SQL 注入漏洞（CNVD-2019

-03304）、多款 Apple 产品 SQLite 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/

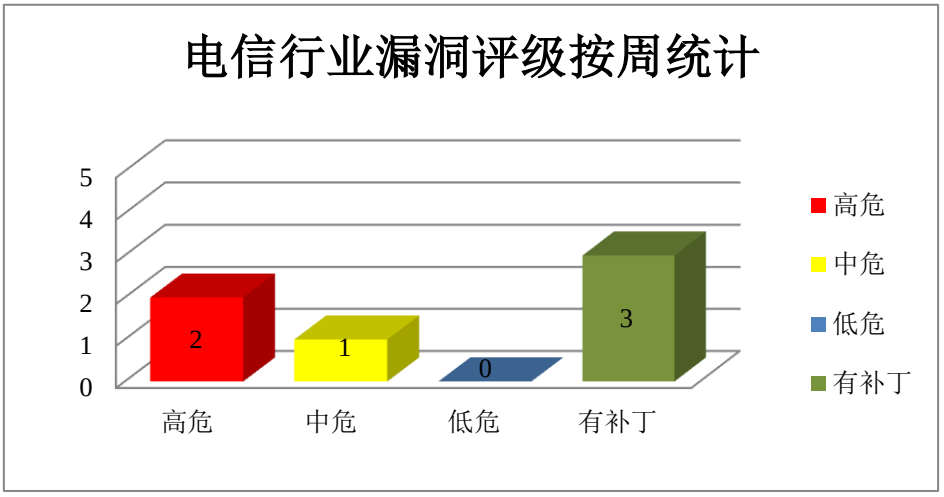

图 3 电信行业漏洞统计

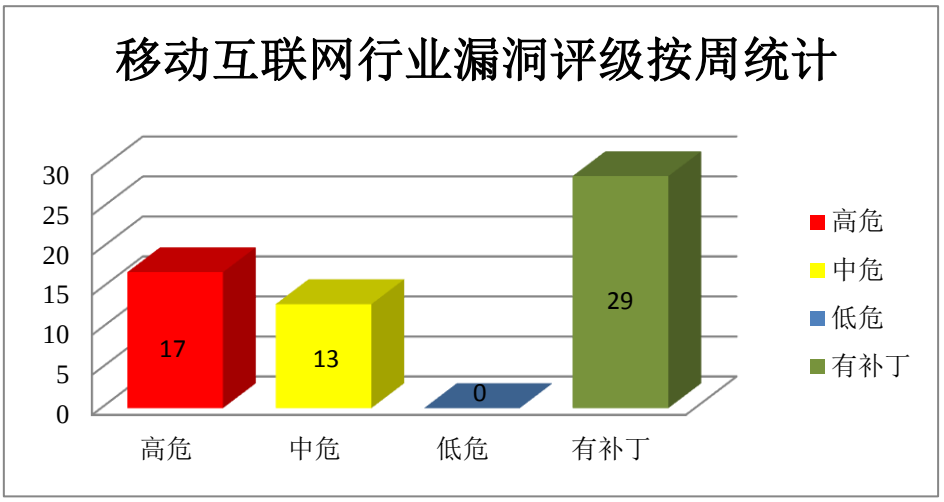

图 4 移动互联网行业漏洞统计

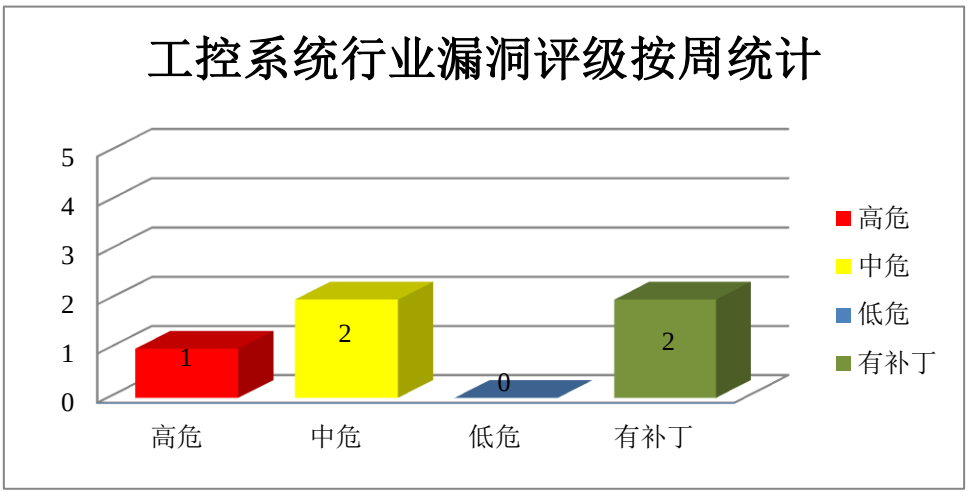

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是美国谷歌（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，上述产品被披露存在权限提升和拒绝服务漏洞，攻击者可利用漏洞提升权限，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android System 权限提升漏洞（CNVD-2019-03705、CNVD-2019-03707、CNVD-2019-03706、CNVD-2019-03708）、Google Android System 组件权限提升漏洞（CNVD-2019-03702、CNVD-2019-03709、CNVD-2019-03710、CNVD-2019-03711）。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-2019-03705
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03707
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03706
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03708
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03702
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03709
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03710
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03711

2、Apple 产品安全漏洞

Apple iOS 为移动设备所开发的一套操作系统；macOS High Sierra 是为 Mac 计算机所开发的一套专用操作系统；tvOS 是一套智能电视操作系统。Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。watchOS 是一套智能手表操作系统。iCloud for Windows 是一款基于 Windows 平台的云服务。本周，上述产品被披露存在缓冲区溢出和内存破坏漏洞，攻击者可利用漏洞执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：多款 Apple 产品 FaceTime 缓冲区溢出漏洞、多款 Apple 产品 Kernel 缓冲区溢出漏洞、多款 Apple 产品 SQLite 内存破坏漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-03295、CNVD-2019-03296、CNVD-2019-03315、CNVD-2019-03316、CNVD-2019-03317）。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-2019-03283
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03288

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03292

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03295

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03296

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03315

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03316

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03317

3、HDF5 产品安全漏洞

HDF5 是一套免费的用于管理存储不同类型数据的工具套件，它能够管理、操作、查看、分析数据，并生成可移植格式的文件。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堆缓冲区越界读取，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：HDF5 缓冲区越界读取漏洞、HDF5 空指针解引用漏洞（CNVD-2019-03443）、HDF5 越界读取漏洞（CNVD-2019-03449）、HDF5 拒绝服务漏洞、HDF5 缓冲区溢出漏洞（CNVD-2019-03450、CNVD-2019-03453、CNVD-2019-03454、CNVD-2019-03455）。目前，互联网上已经出现了针对上述漏洞的攻击代码，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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-03441

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03443

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03449

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03448

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03450

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03453

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03454

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03455

4、HPE 产品安全漏洞

HPE Intelligent Management Center（iMC）是一套网络智能管理中心解决方案。HPE RESTful Interface Tool 是一套可配置、清查和监控各种系统和服务器组件的 RESTful 界面工具，它支持通过命令工具控制电源、BIOS（传统/UEFI）和 iLO 4 设置、读取事件日志等，并提供远程身份验证、脚本部署服务器等功能。HPE StorageWorks XP7 Automation Director（AutoDir）是一款 StorageWorks 自动化管理系统。HPE Integrated Lights-Out 4（iLO 4）和 Integrated Lights-Out 5（iLO 5）都是美国惠普企业（Hewlett Packard Enterprise，HPE）公司的内嵌式服务器管理技术，它通过一个集成的远程管理端口，监视和维护服务器的运行状况、远程管控服务器等。HPE Network Function Virtualization Director（NFVD）是一套 NFV 协调解决方案。HPE CentralView Fraud Risk Management 是一套用于解决欺诈控制问题的端到端解决方案。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，执行任意代码等。

CNVD 收录的相关漏洞包括：HPE Intelligent Management Center 远程代码执行漏洞（CNVD-2019-03320）、HPE RESTful Interface Tool 权限访问控制漏洞、HPE XP7 Automation Director 身份验证绕过漏洞、HPE Integrated Lights Out 4 和 5 for Gen 拒绝服务漏洞、HPE Intelligent Management Center PLAT 代码执行漏洞、HPE Network Function Virtualization Director 信息泄露漏洞、HPE CentralView Fraud Risk Management 信息泄露漏洞、HPE CentralView Fraud Risk Management 未授权访问漏洞。其中，除“HPE Network Function Virtualization Director 信息泄露漏洞、HPE CentralView Fraud Risk Management 信息泄露漏洞、HPE CentralView Fraud Risk Management 未授权访问漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-03320

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03323

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03324

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03321

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03325

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03326

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03327

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03328

5、Technicolor DPC3928SL 跨站脚本漏洞

Technicolor DPC3928SL 是一款电缆调制解调器。本周，Technicolor DPC3928SL 被披露存在跨站脚本漏洞。远程攻击者可借助 setSSID 利用该漏洞注入任意的 Web 脚本或 HTML。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-2019-03479

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-2019-03110	Magento 任意文件读取漏洞	高	升级到 Magento2.3.0 版本：https://magento.com/tech-resources/download
CNVD-2019-03261	Phoenix Contact FL SWITCH 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.phoenixcontact.com
CNVD-2019-03271	Logisim Evolution XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://github.com/reds-heig/logisim-evolution/releases
CNVD-2019-03277	Synology DiskStation Manager 不当转义中和漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.com/zh-cn/security/advisory/Synology_SA_18_14
CNVD-2019-03289	多款 Apple 产品 Kernel 越界读取漏洞	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.apple.com/zh-cn/HT209443
CNVD-2019-03434	EVLink Parking 代码注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-354-01-EVLink.pdf&p_Doc_Ref=SEVD-2018-354-01
CNVD-2019-03457	Micro Focus ArcSight Management Center 跨站请求伪造漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03245142#
CNVD-2019-03464	IIoT Monitor 危险类型文件上传漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-354-03-IIoT+Monitor.pdf&p_Doc_Ref=SEVD-2018-354-03
CNVD-2019-03467	EVLink Parking 提权漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-354-01-EVLink.pdf&p_Doc_Ref=SEVD-2018-354-01
CNVD-2019-03583	QEMU 缓冲区溢出漏洞（CNVD-2019-03583）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.qemu.org/

小结：本周，Google 被披露存在权限提升和拒绝服务漏洞，攻击者可利用漏洞提升权限，造成拒绝服务。此外，Apple、HDF5、HPE 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（内存破坏），造成堆缓冲区越界读取，发起拒绝服务攻击等。另外，Technicolor DPC3928SL 被披露存在跨站脚本漏洞。远程

攻击者可借助 setSSID 利用该漏洞注入任意的 Web 脚本或 HTML。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、Microsoft Windows .CONTACT File / HTML Injection Mailto:远程代码执行漏洞

验证描述

Microsoft Windows 是一款流行的操作系统。

Microsoft Windows .CCT File / HTML Injection Mailto:存在远程代码执行漏洞。允许远程攻击者在易受攻击的 Microsoft Windows 安装上执行任意代码。

验证信息

POC 链接：https://seclists.org/fulldisclosure/2019/Jan/57

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-03281

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. 苹果曝出 FaceTime 电话窃听漏洞

近日，国内外媒体纷纷报道称苹果 FaceTime 存在一个重大漏洞，如果通过 FaceTime 打电话给别人，可利用这个漏洞，在对方接听或拒绝来电之前，通过手机监听到对方的声音。

参考链接：https://www.freebuf.com/news/195316.html

2. Numpy 反序列化命令执行漏洞(CVE-2019-6446)

NumPy 是一个功能强大的 Python 库，主要用于对多维数组执行计算。Numpy 存在反序列化命令执行漏洞。漏洞点位于 npyio.py 的第 268 行，file 字符串对象经过格式验证，允许用户加载恶意数据源造成命令执行。

参考链接：https://www.freebuf.com/vuls/194540.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