国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 02 月 18 日-2019 年 02 月 24 日 **2019 年第 8 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 194 个，其中高危漏洞 48 个、中危漏洞 127 个、低危漏洞 19 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 37 个（占 19%），其中互联网上出现“HotelDruid 跨站脚本漏洞、LibRaw 'copy_bayer'函数空指针逆向引用漏洞”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 2374 个，与上周（1058 个）环比增长 1.24 倍。

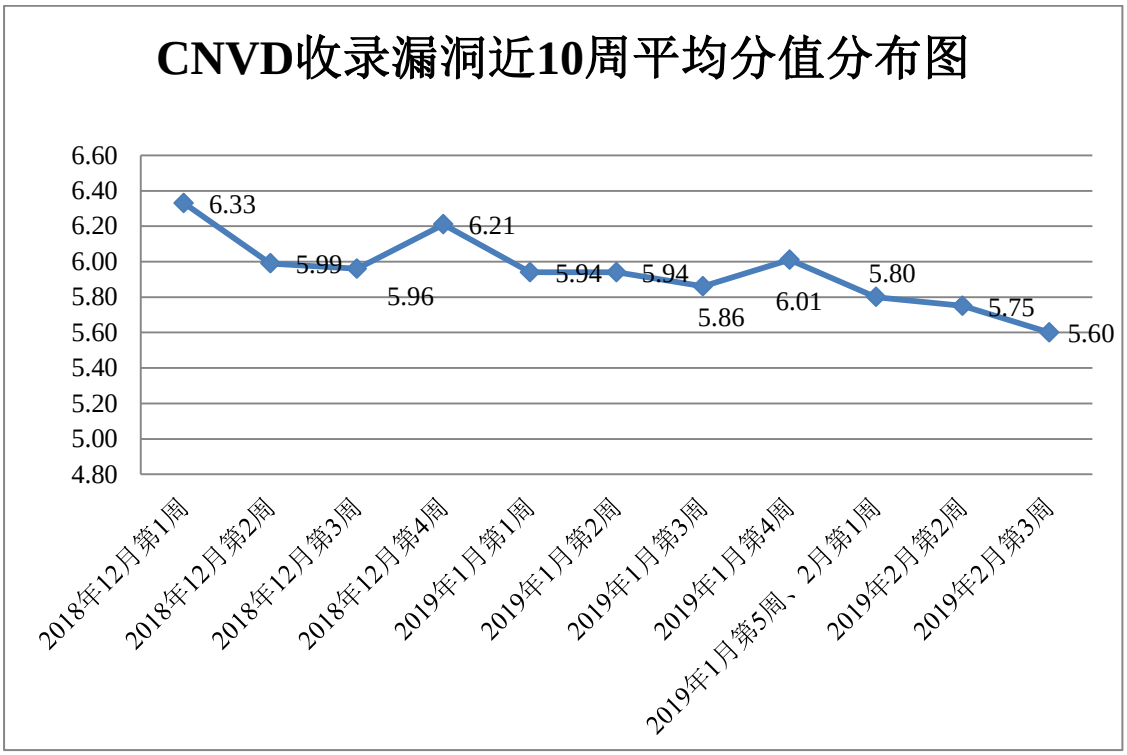

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 3 起，向银行、保险、能源等重要行业

单位通报漏洞事件 39 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 253 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 77 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 20 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：

福建福昕软件开发股份有限公司、合优公司、山西先启科技有限公司、聊城鼎祥网络有限公司、长沙泽帆网络科技有限公司、锐步网络科技有限公司、淄博闪灵网络科技有限公司、康智达数字技术有限公司、河南汉申网络科技有限公司、济南锐步网络科技有限公司、长沙米拓信息技术有限公司、嘉兴想天信息科技有限公司、郑州擎天科技有限公司、北京网盟信息技术发展有限公司、得实信息科技（深圳）有限公司、启明星工作室、今日看点、环保时代网、中国电子政务网、Jeeplus 社区、大米 CMS、帝国软件、海纳网络工作室、中国消费者协会和海洋 CMS。

本周，CNVD 发布了《关于 WinRAR 存在系列远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4903

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、华为技术有限公司、中国电信集团系统集成有限责任公司、北京数字观星科技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、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、山东华鲁科技发展股份有限公司、山东云天安全技术有限公司、重庆贝特计算机系统工程有限公司、南京联成科技发展股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、内蒙古奥创科技有限公司、山石网科通信技术股份有限公司、北京国舜科技股份有限公司、河南信安世纪科技有限公司及其他个人白帽子向 CNVD 提交了 2374 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 1718 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）	1177	1177
360 网神（补天平台）	541	541
哈尔滨安天科技集团股份有限公司	158	0

北京天融信网络安全技术有限公司	123	21
华为技术有限公司	97	0
中国电信集团系统集成有限责任公司	92	4
北京数字观星科技有限公司	91	0
北京神州绿盟科技有限公司	84	0
北京启明星辰信息安全技术有限公司	72	2
新华三技术有限公司	61	0
四川无声信息技术有限公司	37	37
北京知道创宇信息技术有限公司	12	0
厦门服云信息科技有限公司	12	0
恒安嘉新(北京)科技股份公司	8	0
杭州安恒信息技术股份有限公司	2	2
沈阳东软系统集成工程有限公司	1	1
天津市国瑞数码安全系统股份有限公司	168	168
中新网络信息安全股份有限公司	66	66
任子行网络技术股份有限公司	64	64
安徽锋刃信息科技有限公司	55	55
山东华鲁科技发展股份有限公司	31	31
山东云天安全技术有限公司	30	30
重庆贝特计算机系统工程有限公司	10	10
南京联成科技发展股份有限公司	9	9
远江盛邦（北京）网络安全科技股份有限公司	8	8

内蒙古奥创科技有限公司	4	4
山石网科通信技术股份有限公司	2	2
北京国舜科技股份有限公司	1	1
河南信安世纪科技有限公司	1	1
CNCERT 甘肃分中心	8	8
CNCERT 吉林分中心	6	6
CNCERT 湖南分中心	5	5
CNCERT 上海分中心	4	4
CNCERT 贵州分中心	3	3
CNCERT 天津分中心	3	3
CNCERT 海南分中心	1	1
CNCERT 广东分中心	1	1
个人	109	109
报送总计	3157	2374

本周漏洞按类型和厂商统计

本周，CNVD 收录了 194 个漏洞。应用程序漏洞 150 个，WEB 应用漏洞 24 个，操作系统漏洞 11 个，网络设备漏洞 8 个，安全产品漏洞 1 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	150
WEB 应用漏洞	24
操作系统漏洞	11
网络设备漏洞	8
安全产品漏洞	1

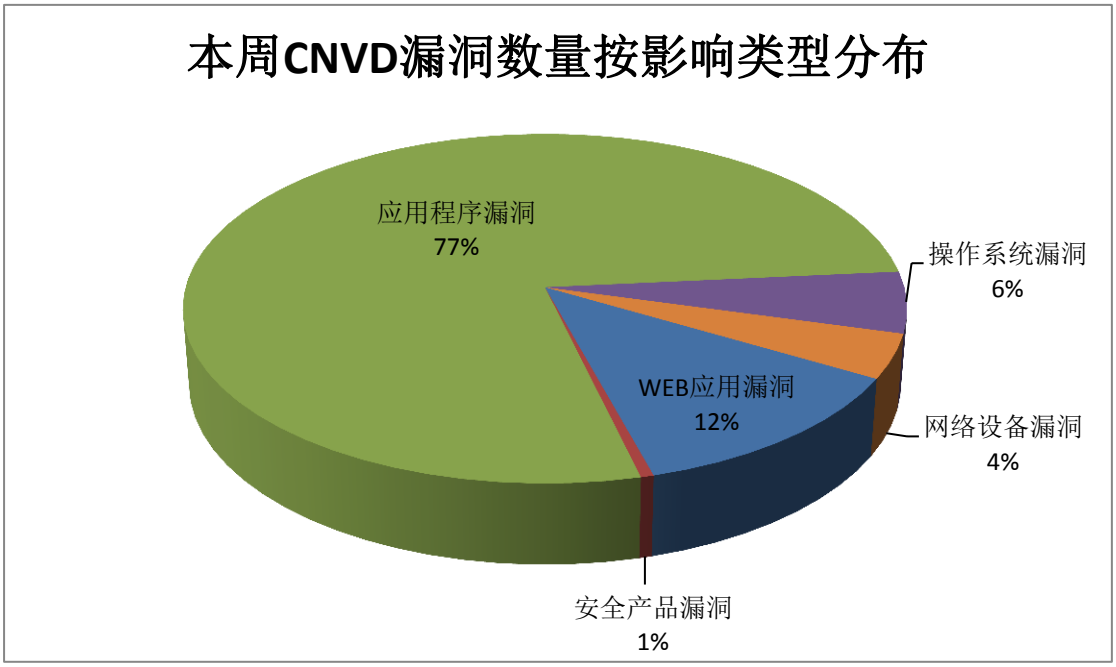

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SAP、LibRaw、LibVNC 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	SAP	31	16%
2	LibRaw	20	10%
3	LibVNC	12	6%
4	Qemu	12	6%
5	Zoneminder	11	6%
6	Schneider Electric	9	5%
7	Apple	9	5%
8	Cisco	8	4%
9	Foxit	8	4%
10	其他	74	38%

本周行业漏洞收录情况

本周，CNVD 收录了 3 个电信行业漏洞，18 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI 代码执行漏洞、Apple iOS、tvOS 和 macOS libxpc 任意代码执行漏洞、Schneider

Electric Modicon M221 远程安全绕过漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-04711）”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/

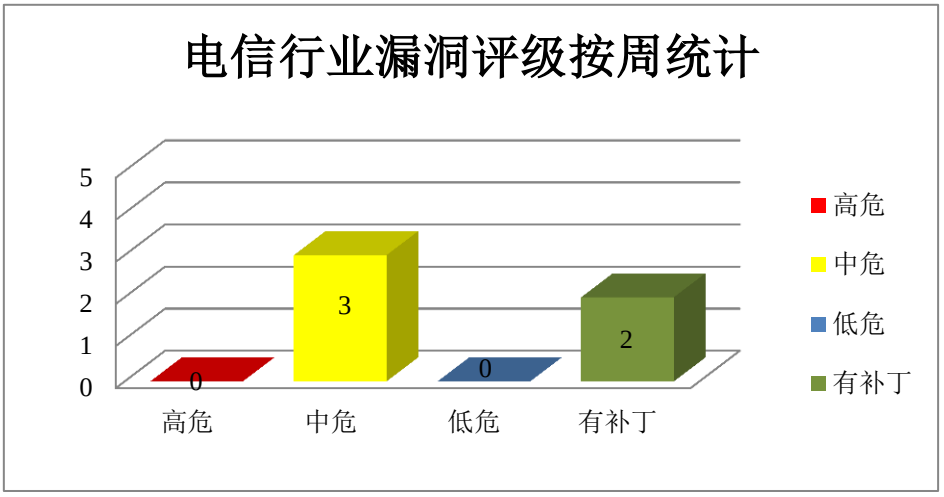

图 3 电信行业漏洞统计

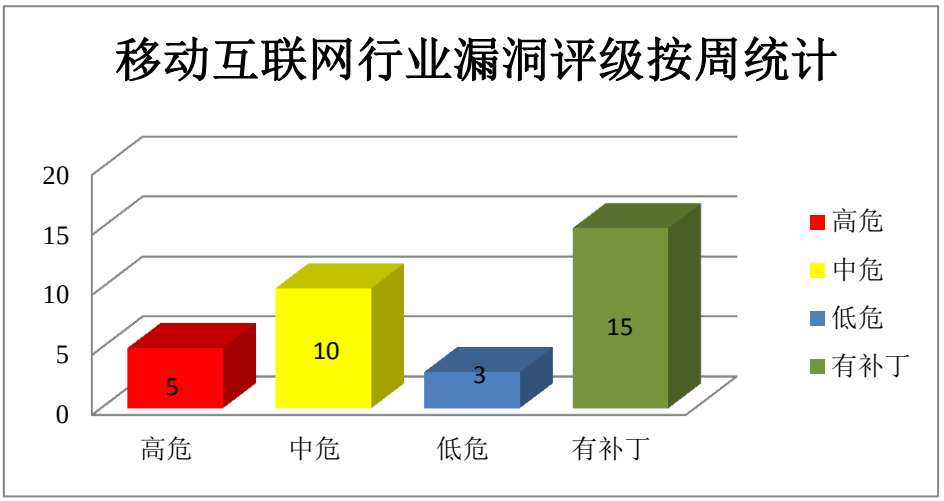

图 4 移动互联网行业漏洞统计

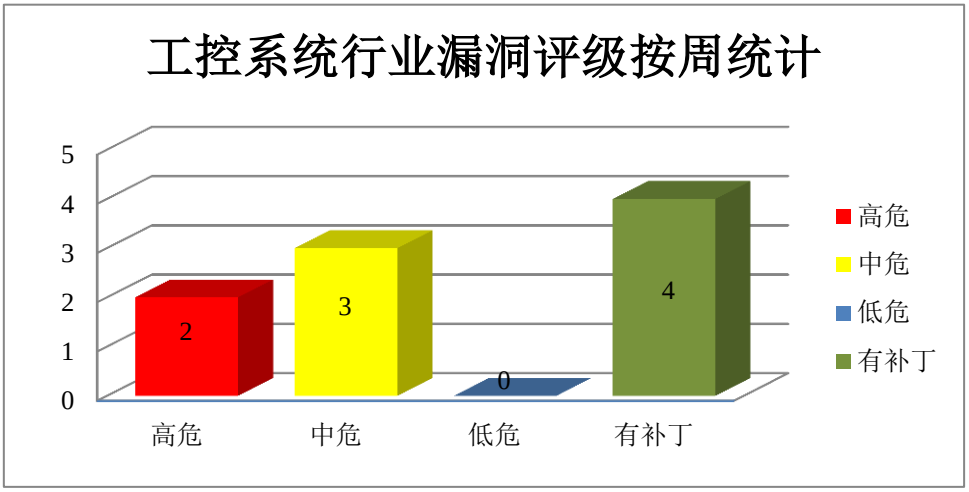

图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco TelePresence Management Suite 是一款视频服务器管理程序。Cisco Firepower Management Center 是一款设备管理应用。Cisco TelePresence Video Communication Server 是一款视频服务器。Cisco Web Security Appliance 是一款 WEB 安全访问设备。Cisco SPA112 Series 是一款 SPA112 系列 IP 电话。SPA525 Series 是一款 SPA525 系列 IP 电话。SPA5X5 Series 是一款 SPA5X5 系列 IP 电话。Cisco Firepower Threat Defense（FTD）是一套提供下一代防火墙服务的统一软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，绕过 DROP 策略，进行未授权访问，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco TelePresence Management Suite SOAP 未授权访问漏洞、Cisco Firepower Management Center 跨站脚本漏洞（CNVD-2019-04919）、Cisco TelePresence Video Communication Server (VCS)跨站请求伪造漏洞、Cisco TelePresence Management Suite 跨站脚本漏洞（CNVD-2019-04920）、Cisco Web Security Appliance 安全绕过漏洞、Cisco SPA112、SPA525 和 SPA5X5 Series 证书验证漏洞、Cisco Network Convergence System 1000 Series IOS XR Software 信息泄露漏洞、Cisco Firepower Threat Defense 输入验证漏洞。其中，“Cisco Network Convergence System 1000 Series IOS XR Software 信息泄露漏洞”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-2019-04918

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04919

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04922

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04920

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04921

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04936

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04942

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04943

2、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；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。iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。WebKit 是其中的一个 Web 浏览器引擎组件。tvOS 是一套智能电视操作系统；OS X El Capitan 是一套专为 Mac 计算机所开发的专用操作系统。watchOS 是一套智能手表操作系统；macOS High Sierra 是为 Mac 计算机所开发的一套专用操作系统。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，执行任意代码（内存破坏），造成 ASSERT 失败。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 断言失败漏洞（CNVD-2019-04706、CNVD-2019-04707）、Apple iOS、tvOS 和 OS X El Capitan CFNetwork Proxies 信息泄露漏洞、多款 Apple 产品 CoreGraphics 越界读取漏洞、多款 Apple 产品 Kernel 远程代码执行漏洞、多款 Apple 产品 Kernel 信息泄露漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-04711）、Apple iOS、tvOS 和 macOS libxpc 任意代码执行漏洞。其中，“多款 Apple 产品 Kernel 远程代码执行漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-04711）、Apple iOS、tvOS 和 macOS libxpc 任意代码执行漏洞”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-2019-04706

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04707

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04705

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04708

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04709

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04710

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04711

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04945

3、Schneider Electric 产品安全漏洞

Schneider Electric Pelco Sarix Professional 1st generation cameras 是一款 IP 摄像机设备。Schneider Electric Evlink Charging Station 是一套商用电动汽车充电解决方案。Schneider Electric Wiser for KNX、homeLYnk 和 spaceLYnk 都是法国施耐德电气（Schneider Electric）公司的用于不同逻辑控制器的自动化编程软件。Schneider Electric So

Machine Basic 是一款用于在控制平台上对元器件进行编程、调试的软件。Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI（前称 InTouch Machine Edition）都是法国施耐德电气（Schneider Electric）公司的嵌入式 HMI 软件包。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞查看明文形式的密码，获取未授权访问权限，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：Schneider Electric Pelco Sarix Professional 1st generation cameras 缓冲区溢出漏洞、Schneider Electric Pelco Sarix Professional 1st generation cameras 权限提升漏洞、Schneider Electric Evlink Charging Station 权限提升漏洞、Schneider Electric Wiser for KNX、homeLYnk 和 spaceLYnk 未经授权访问漏洞、Schneider Electric SoMachine Basic XML 外部实体注入漏洞、Schneider Electric Modicon M221 远程安全绕过漏洞、Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI 代码执行漏洞、Schneider Electric Pelco Sarix Professional 1st generation cameras 身份验证密码泄露漏洞。其中，“Schneider Electric Pelco Sarix Professional 1st generation cameras 缓冲区溢出漏洞、Schneider Electric Evlink Charging Station 权限提升漏洞、Schneider Electric Modicon M221 远程安全绕过漏洞、Schneider Electric InduSoft Web Studio 和 InTouch Edge HMI 代码执行漏洞”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-2019-05103

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05104

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05105

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05106

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05109

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05108

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05107

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05110

4、SAP 产品安全漏洞

SAP HANA 是一套高性能的实时数据分析平台。Extended Application Services 是一个应用程序服务器、Web 服务器和 SAP HANA System 内 Web 应用的开发环境。SAP Cloud Connector 是一款用于连接 SAP 云平台的连接器。SAP BusinessObjects Business Intelligence Platform 是一套商务智能软件和企业绩效解决方案套件。SAP Cloud Connector 是一款用于连接 SAP 云平台的连接器。SAP Landscape Management 是一套业务流程解决方案。SAP ABAP Application Server 是一款 Web 应用程序服务器。Gateway 是其中的一个连接 SAP 软件与设备、环境和平台的框架。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，执行未授权的操作，上传任意文件，执行任

意代码。

CNVD 收录的相关漏洞包括：SAP HANA Extended Application Service 信息泄露漏洞、SAP Cloud Connector 代码注入漏洞、SAP BusinessObjects Business Intelligence Platform 任意文件上传漏洞、SAP Cloud Connector 授权问题漏洞、SAP Landscape Management 信息泄露漏洞（CNVD-2019-04859）、SAP ABAP Application Server Gateway 信息泄露漏洞、SAP Adaptive Server Enterprise 信息泄露漏洞（CNVD-2019-05032、CNVD-2019-05056）。其中，“SAP Cloud Connector 代码注入漏洞、SAP BusinessObjects Business Intelligence Platform 任意文件上传漏洞、SAP Cloud Connector 授权问题漏洞”的综合评级为“高危”。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：http://www.cnvd.org.cn/flaw/show/CNVD-2019-04851

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04855

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04857

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04861

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04859

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04893

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05032

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05056

5、Thinkphp 'Request.php'文件代码执行漏洞

ThinkPHP 是由上海顶想信息科技有限公司开发维护的 MVC 结构的开源 PHP 框架。本周，Thinkphp 'Request.php'文件被披露存在代码执行漏洞。攻击者利用该漏洞对目标网站进行远程命令执行攻击。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-2019-04930

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-2019-04453	Invision Power Board 存储型跨站脚本漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：http://invision-virus.com/forum/index.php/files/file/1080-ipboardv349-illusion-nulled-with-calendar/
CNVD-2019-04687	ZoneMinder SQL 注入漏洞（CNVD-2019-04687）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://zoneminder.com/
CNVD-2019-04703	Foxit Reader 和 PhantomPDF for Windows 验证绕过漏洞	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.foxitsoftware.com/support/security-bulletins.php
CNVD-2019-04909	Drupal Core 远程代码执行漏洞（CNVD-2019-04909）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.drupal.org/sa-core-2019-002
CNVD-2019-04910	WinRAR LHA/LZH 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.win-rar.com/whatsnew.html
CNVD-2019-04911	WinRAR ACE 文件验证逻辑绕过漏洞	高	WinRAR 厂商已发布新版本修复此漏洞，建议立即升级至最新版本：https://www.win-rar.com/download.html
CNVD-2019-04912	WinRAR ACE 文件名逻辑验证绕过漏洞	高	WinRAR 厂商已发布新版本修复此漏洞，建议立即升级至最新版本：https://www.win-rar.com/download.html
CNVD-2019-04913	WinRAR ACE/RAR 任意代码执行漏洞	高	WinRAR 厂商已发布新版本修复此漏洞，建议立即升级至最新版本：https://www.win-rar.com/download.html
CNVD-2019-05064	LibRaw 'parse_minolta()'函数拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.suse.com/support/update/announcement/2018/suse-su-20183343-1/
CNVD-2019-05085	QEMU 'qemu_deliver_packet_iov'函数拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.qemu.org/

小结：本周，Cisco 被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，绕过 DROP 策略，进行未授权访问，造成拒绝服务等。此外，Apple、Schneider Electric、SAP 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，执行未授权的操作，提升权限，上传任意文件，执行任意代码或造成拒绝服务等。另外，Thinkphp 'Request.php'文件被披露存在代码执行漏洞。攻击者利用该漏洞对目标网站进行远程命令执行攻击。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、LibRaw 'copy_bayer'函数空指针逆向引用漏洞

验证描述

LibRaw 是一个用来处理 RAW(CRW/CR2、NEF、RAF、DNG 和 others)格式图片的 C++库。

LibRaw 0.19.1 版本中的 libraw_cxx.cpp 文件的'copy_bayer'函数存在空指针逆向引用漏洞。攻击者可利用该漏洞造成拒绝服务（崩溃和段错误）。

验证信息

POC 链接：https://github.com/LibRaw/LibRaw/issues/194

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-05077

信息提供者

华为技术有限公司

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. 微软发布安全警告：Windows Sever 容易受到 DoS 攻击

近日微软在安全响应中心发布安全警告，称 Windows Sever 和 Windows 10 server 都容易受到 DoS 攻击。具体说来，所有运行 IIS（互联网信息服务）的 Windows Server 2016、Windows Server Version 170、Windows Server Version 1803 以及 Windows 10 (1607、1703、1709 和 1803 版本)都会受遭遇该 DoS 攻击。这主要是因为 ISS 中存在资源耗尽 bug，会触发 DoS 条件，被潜在的远程攻击者利用。这个 bug 会“临时导致系统 CPU 使用率蹿升至 100%，直到恶意链接遭 IIS 杀死。”微软在安全通告中指出，目前尚未有针对该漏洞（由 F5 Networks 公司研究员 Gal Goldshtein 报告）的缓解措施或变通措施。并建议用户参考二月份的非安全更新建议，及时更新以确保安全。

参考链接：https://www.bleepingcomputer.com/news/security/windows-servers-vulnerable-to-iis-resource-exhaustion-dos-attacks/

2. WinRAR 被曝存在遗留 19 年的漏洞，影响全球多达 5 亿用户

根据 Check Point 研究人员的说法，该问题是因 UNACEV2.dll 代码库中的一个深藏已久的漏洞引起的，而且该代码库从 2005 年以来就一直没有被主动使用过。据了解，该代码库用于解析 ACE 格式，这是一种可以追溯到 20 世纪 90 年代常用的压缩格式。攻击者可以制作一个恶意的 ACE 文件，当被 WinRAR 打开的时候，会利用 UNACEV2.dll 中的路径遍历漏洞欺骗归档工具将文件解压到攻击者选择的路径中。研究人员试图将 ACE 恶意文件放到启动文件夹中以便在系统启动时执行。

参考链接：https://research.checkpoint.com/extracting-code-execution-from-winrar/

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