国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 09 月 09 日-2019 年 09 月 15 日 **2019 年第 37 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 365 个，其中高危漏洞 87 个、中危漏洞 253 个、低危漏洞 25 个。漏洞平均分值为 5.87。本周收录的漏洞中，涉及 0day 漏洞 79 个（占 22%），其中互联网上出现“iF.SVNAdmin 跨站请求伪造漏洞、Best Soft Inc.（BSI）Advance Hotel Booking System 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 2276 个，与上周（3140 个）环比降低 28%。

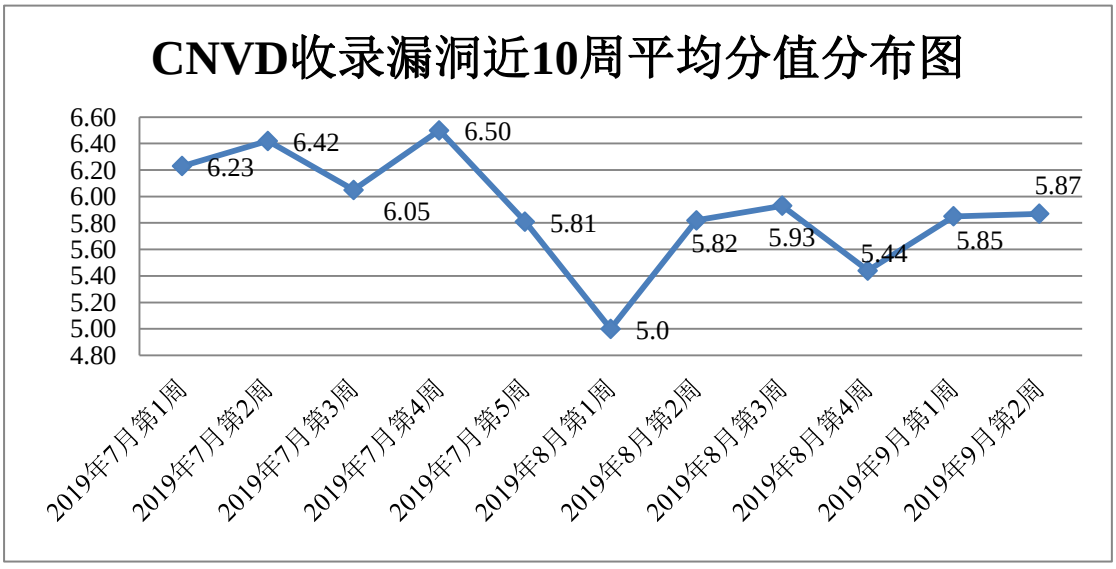

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 0 起，向银行、保险、能源等重要行业单位通报漏洞事件 5 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 172 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 39 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14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、杭州云霁科技有限公司、青岛网搜网络技术有限公司、桂林崇胜网络科技有限公司、卫宁健康科技集团股份有限公司、湖南三唐信息科技有限公司、深圳市小水滴计算机系统有限公司、深圳市蓝凌软件股份有限公司、深圳迪元素科技有限公司、上海晓材科技有限公司、深圳市锟铻科技有限公司、深圳市正达自动化系统有限公司、四川迅睿云软件开发有限公司、青岛飞鸽软件有限公司、中达电通股份有限公司、上海卓卓网络科技有限公司、三菱电机自动化（中国）有限公司、北京亿赛通科技发展有限责任公司、广东凯格科技有限公司、河南网中网计算机科技有限公司、中电科新型智慧城市研究院有限公司、山西美丽通行科技有限公司、南京苏迪科技有限公司、民生置业有限公司、中粮集团有限公司、昆明奥远科技有限公司、长沙米拓信息技术有限公司、苏州恩斯特网络科技有限公司、江苏楚淮软件科技开发有限公司、睿谷信息科技、中国岩石力学与工程学会地下空间分会、六安市开发区鹏程网络工作室、中国机械工业联合会、中国银行间市场交易商协会、SchoolCMS、鱼跃 CMS、Zzzcms、MoMoCMS、CatfishCMS 和 HadSky。

本周，CNVD 发布了《Microsoft 发布 2019 年 9 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5205

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、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。南京众智维信息科技有限公司国网思极检测技术（北京）有限公司山东新潮信息技术有限公司任子行网络技术股份有限公司北京天地和兴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君信安科技有限公司上海银基信息安全技术股份有限公司广州锦行网络科技有限公司北京铭图天成信息技术有限公司河南信安世纪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上海并擎软件科技有限公司及其他个人白帽子向 CNVD 提交了2276 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）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 1862 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）	899	899
奇安信网神（补天平台）	689	689
上海交大	274	274
北京天融信网络安全技术有限公司	236	14
哈尔滨安天科技集团股份有限公司	204	0
华为技术有限公司	146	0
深信服科技股份有限公司	87	0
北京神州绿盟科技有限公司	79	6
新华三技术有限公司	44	0
北京启明星辰信息安全技术有限公司	44	0
恒安嘉新(北京)科技股份公司	39	0
北京数字观星科技有限公司	21	0
中新网络信息安全股份有限公司	8	8
北京知道创宇信息技术股份有限公司	5	3
沈阳东软系统集成工程有限公司	1	1
南京众智维信息科技有限公司	92	92
国网思极检测技术（北京）有限公司	56	56
山东新潮信息技术有限公司	44	44
任子行网络技术股份有限公司	17	17
北京天地和兴科技有限公司	16	16
远江盛邦（北京）网络安全科技股份有限公司	14	14
北京君信安科技有限公司	10	10

上海银基信息安全技术股份有限公司	9	9
广州锦行网络科技有限公司	8	8
北京铭图天成信息技术有限公司	4	4
河南信安世纪科技有限公司	3	3
北京智游网安科技有限公司	2	2
北京信联科汇科技有限公司	2	2
上海并擎软件科技有限公司	1	1
CNCERT 四川分中心	5	5
CNCERT 贵州分中心	1	1
个人	98	98
报送总计	3158	2276

本周漏洞按类型和厂商统计

本周，CNVD 收录了 365 个漏洞。WEB 应用 132 个，应用程序 164 个，操作系统 47 个，网络设备（交换机、路由器等网络端设备）14 个，智能设备（物联网终端设备）漏洞 3 个，安全产品 3 个，数据库 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
WEB 应用	132
应用程序	164
操作系统	47
网络设备（交换机、路由器等网络端设备）	14
智能设备（物联网终端设备）漏洞	3
安全产品	3
数据库	2

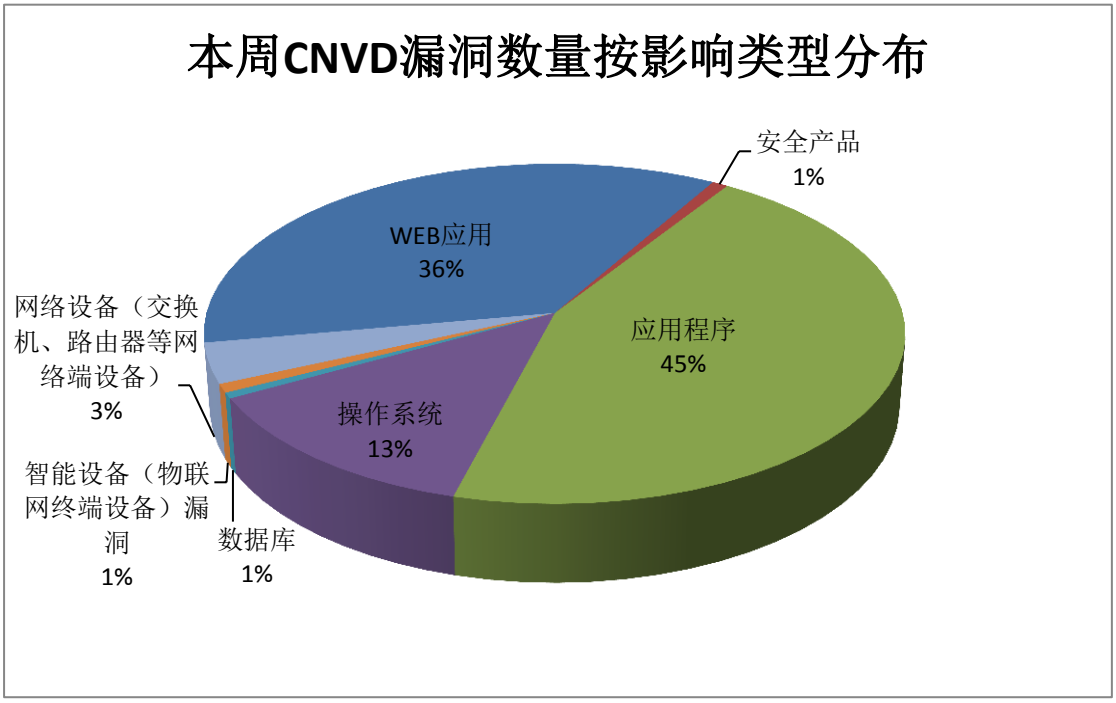

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Adobe、Google 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	WordPress	98	27%
2	Adobe	23	7%
3	Google	22	6%
4	Limesurvey	19	5%
5	Oracle	18	5%
6	IBM	12	3%
7	Microsoft	11	3%
8	VideoLAN	10	2%
9	Cisco	8	2%
10	其他	144	40%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，29 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“TP-Link M7350 V3 命令注入漏洞（CNVD-2019-31307）、TP-Link M7350 V3 命令注入漏洞、PostgreSQL 存在未明漏洞”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/

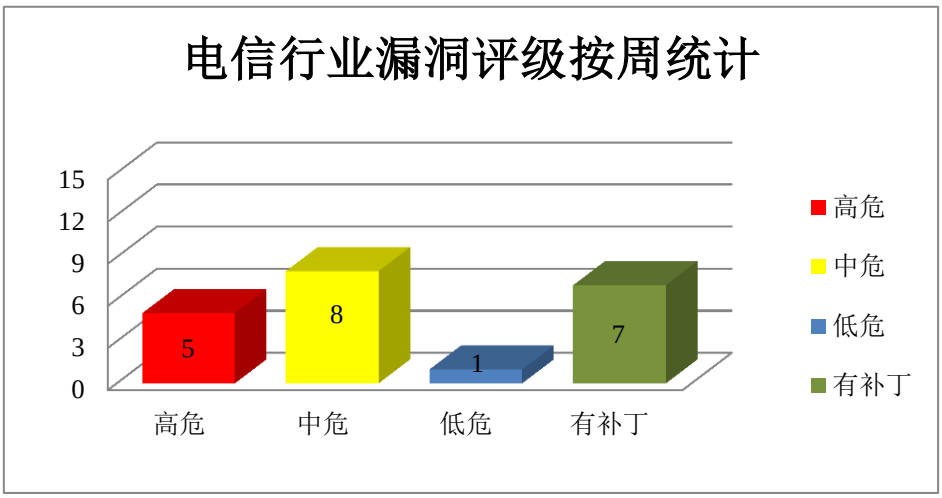

图 3 电信行业漏洞统计

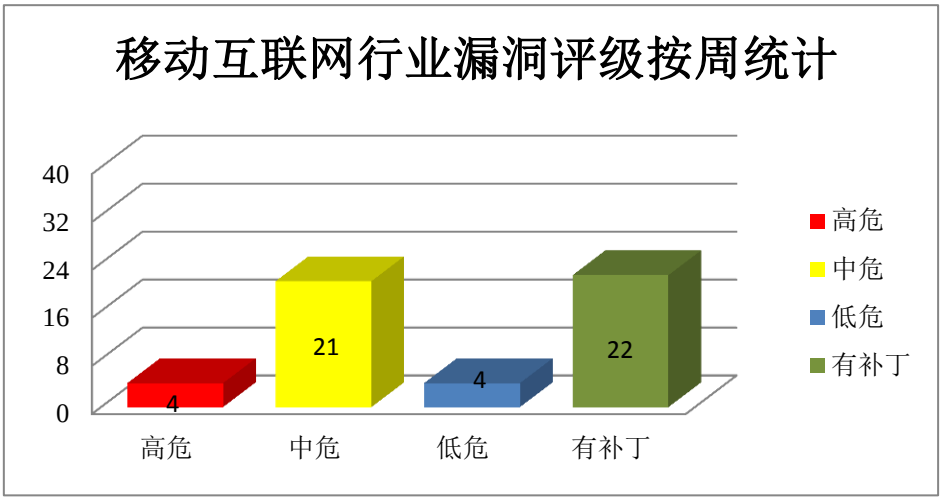

图 4 移动互联网行业漏洞统计

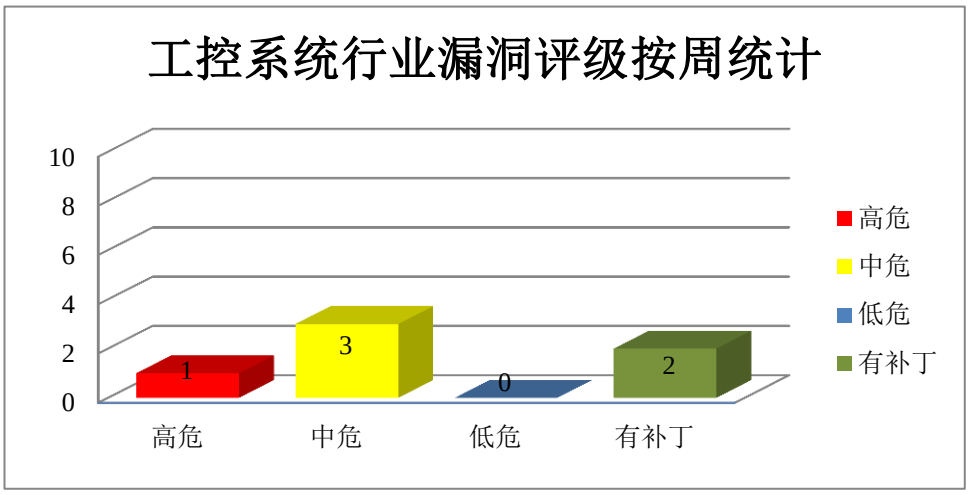

图 5 工控系统行业漏洞统计

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）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。System 是其中的一个系统组件。本周，该产品被披露存在信息泄露漏洞，攻击者可利用漏洞获取受影响组件敏感信息。

CNVD 收录的相关漏洞包括：Google Android System 信息泄露漏洞（CNVD-2019-31033、CNVD-2019-31034、CNVD-2019-31035、CNVD-2019-31036、CNVD-2019-31037、CNVD-2019-31038、CNVD-2019-31041、CNVD-2019-31042）。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-2019-31033
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31034
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31035
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31036
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31037
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31038
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31041
http://www.cnvd.org.cn/flaw/show/CNVD-2019-31042

2、Adobe 产品安全漏洞

Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是 Adobe 公司开发的一款 PDF 文件阅读软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取信息或执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 缓冲区溢出漏洞（CNVD-2019-31021、CNVD-2019-31022）、Adobe Acrobat/Reader 不可信指针解引用漏洞（CNVD-2019-30978、CNVD-2019-30979、CNVD-2019-30980、CNVD-2019-30981）、Adobe Acrobat/Reader 整数溢出漏洞（CNVD-2019-31025）、Adobe Acrobat/Reader 数据泄露漏洞。其中，“Adobe Acrobat/Reader 缓冲区溢出漏洞（CNVD-2019-31021、CNVD-2019-31022）、Adobe Acrobat/Reader 不可信指针解引用漏洞（CNVD-2019-30978、CNVD-2019-30979、CNVD-2019-30980、CNVD-2019-30981）”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-2019-31021

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31022

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30978

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30979

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30980

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30981

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31025

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31023

3、GitLab 产品安全漏洞

GitLab 是美国 GitLab 公司的一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。该程序可用于查阅项目的文件内容、提交历史、Bug 列表等。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞绕过项目可视性限制和合并请求的讨论限制，耗尽客户端资源，执行客户端代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：GitLab 跨站脚本漏洞（CNVD-2019-31313）、GitLab 授权问题漏洞（CNVD-2019-31314）、GitLab 拒绝服务漏洞（CNVD-2019-31315、CNVD-2019-31322）、GitLab 限制绕过漏洞（CNVD-2019-31323、CNVD-2019-31324）、GitLab HTML 注入漏洞（CNVD-2019-31316）、GitLab 代码问题漏洞。其中，“GitLab 代码问题漏洞”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-2019-31313

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31314

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31315

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31316

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31317

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31322

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31323

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31324

4、WordPress 产品安全漏洞

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞向服务器发送非预期的请求，执行非法 SQL 命令。

CNVD 收录的相关漏洞包括：WordPress wp-all-import 插件 SQL 注入漏洞、WordPress newsletter-by-supsystic 插件跨站请求伪造漏洞、WordPress wp-business-intelligence-lite 插件 SQL 注入漏洞、WordPress note-press 插件 SQL 注入漏洞、WordPress easy-digital-downloads 插件 SQL 注入漏洞、WordPress 404-to-301 插件 SQL 注入漏洞、WordPress i-recommend-this 插件 SQL 注入漏洞、WordPress visitors-online 插件 SQL 注入漏洞。

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-2019-31133

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31153

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31172

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31173

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31175

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31177

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31178

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31180

5、Xpdf 缓冲区溢出漏洞（CNVD-2019-31202）

Xpdf 是 Foo 实验室的一款开源的 PDF 阅读器。本周，Xpdf 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞导致缓冲区溢出或堆溢出。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-2019-31202

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-2019-30794	Exim 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://exim.org/
CNVD-2019-30907	CA Technologies Client Automation 和 Workload Automation AE 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://techdocs.broadcom.com/us/product-content/recommended-reading/security-notices/CA20190904-01--security-notice-for-ca-common-services-distributed-intelligence-architecture-dia.html
CNVD-2019-31056	Microsoft Windows AppX Deployment Service 提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0841
CNVD-2019-31131	IBM Emptoris Spend Analysis 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://www-01.ibm.com/support/docview.wss?uid=ibm10880223
CNVD-201	PHP pecl-http extension 缓冲	高	厂商已发布了漏洞修复程序，请及时

9-31199	区溢出漏洞		关注更新：https://github.com/m6w6/ext-http/commit/17137d4ab1ce81a2cee0fae842340a344ef3da83
CNVD-2019-31201	Facebook HHVM 缓冲区溢出漏洞（CNVD-2019-31201）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/facebook/hhvm/commit/f9680d21beaa9eb39d166e8810e29fbafa51ad15
CNVD-2019-31230	Silver Peak Systems EdgeConnect SD-WAN 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://github.com/sdnewhop/sdwannewhope/blob/master/reports/Silverpeak%20EdgeConnect%20Multiple%20Vulnerabilities%20-%20032018.pdf
CNVD-2019-31298	Cisco Webex Teams 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190904-webex-teams
CNVD-2019-31312	TP-Link M7350 V3 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://www.tp-link.com/
CNVD-2019-31368	OpenSC 越界访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/OpenSC/OpenSC/commit/a3fc7693f3a035a8a7921cffb98432944bb42740

小结：本周，Google 被披露存在信息泄露漏洞，攻击者可利用漏洞获取受影响组件敏感信息。此外，Adobe、GitLab、WordPress 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞绕过项目可视性限制和合并请求的讨论限制，耗尽客户端资源，执行任意代码或造成拒绝服务等。另外，Xpdf 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞导致缓冲区溢出或堆溢出。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、Best Soft Inc.（BSI）Advance Hotel Booking System 跨站脚本漏洞

验证描述

Best Soft Inc.（BSI）Advance Hotel Booking System 是印度 Best Soft 公司的一套

酒店在线预订系统。该系统提供酒店预订、房间查询和折扣券等模块。

Best Soft Inc. (BSI) Advance Hotel Booking System 2.0 版本中的 booking_details.php 脚本存在跨站脚本漏洞。远程攻击者可借助‘title’参数利用该漏洞注入任意 Web 脚本或 HTML。

验证信息

POC 链接：https://packetstormsecurity.com/files/126949/BSI-Advance-Hotel-Booking-System-2.0-Cross-Site-Scripting.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-31327

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. 网络安全专家称拍照比“剪刀手”会泄露指纹信息

9 月 15 日上午，作为 2019 年国家网络安全宣传周上海地区活动的重要组成部分，“全民体验日”主会场活动在杨浦区创智天地下沉式广场启动。拍照时如果镜头距离够近，“剪刀手”照片通过照片放大技术和人工智能增强技术，就能将照片中人物的指纹信息还原出来。

参考链接：https://www.cnbeta.com/articles/tech/889399.htm

2.谷歌开始收集面部数据 隐私问题再度引爆

谷歌最新的智能显示屏最近出了一项备受争议的新功能 Face Match，它是在谷歌 Nest Hub Max 上推出的。Face Match 使用智能显示屏的前置摄像头作为一项安全功能，以及参与视频通话的一种方式。当它识别出你的脸时，它还会显示你的照片、短信、日历等细节。

参考链接：https://www.cnbeta.com/articles/tech/889141.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