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 16 日-2019 年 09 月 22 日　　2019 年第 38 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 405 个，其中高危漏洞 88 个、中危漏洞 281 个、低危漏洞 36 个。漏洞平均分值为 5.68。本周收录的漏洞中，涉及 0day 漏洞 57 个（占 14%），其中互联网上出现“WordPress quotes-collection 插件跨站脚本漏洞、FlameCMS login.php 文件 SQL 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 2794 个，与上周（2276 个）环比增长 23%。

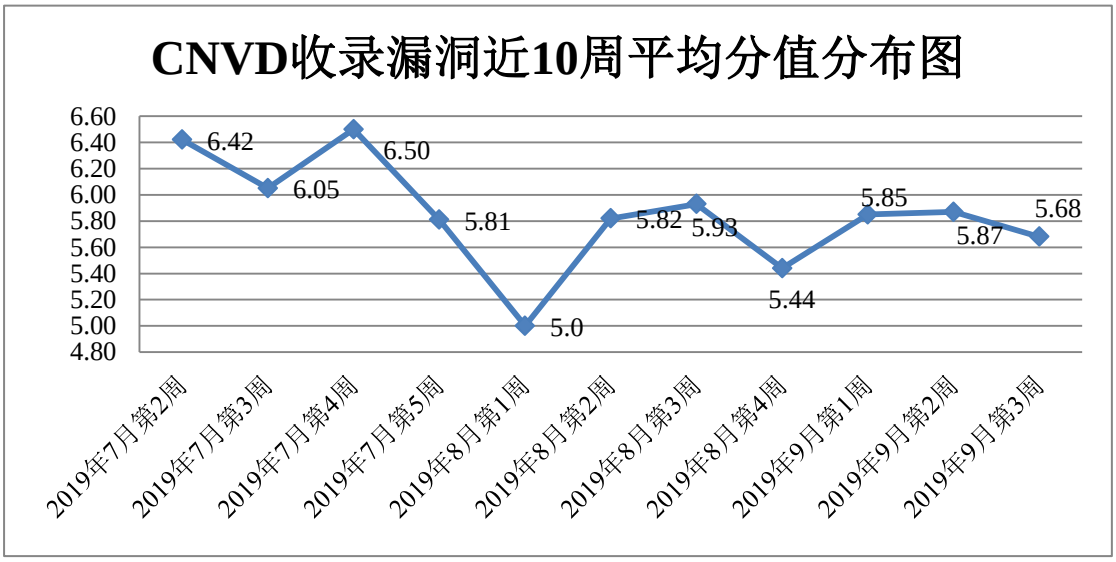

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 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 459 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17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：

杭州艾朴软件有限公司、北京火绒网络科技有限公司、淄博闪灵网络科技有限公司、深圳市昂捷信息技术有限公司、哈尔滨新中新电子股份有限公司、优慕课在线教育科技（北京）有限责任公司、云络电子科技有限公司、成都时代汇创科技有限公司、微软(中国)有限公司、南京本安仪表系统有限公司、上海蒜芽信息科技有限公司、郑州微口网络科技有限公司、南通艾睦网络科技有限公司、广州齐博网络科技有限公司、苏州恩斯特网络科技有限公司、北京智量科技有限公司、海南赞赞网络科技有限公司、四川迅睿云软件开发有限公司、深圳昆仑通态科技有限责任公司、黑龙江金农信息技术有限公司、三菱电机自动化（中国）有限公司、浙江核新同花顺网络信息股份有限公司、大连黎明时代科技发展有限公司、洪湖尔创网联信息技术有限公司、北京网御星云信息技术有限公司、中远海运国际货运有限公司、天津企朋科技发展有限公司、中航出版传媒有限责任公司、常州微诺信息科技有限公司、淄博汇通电子科技有限公司、上海突进网络科技有限公司、北京九州云动科技有限公司、成都力奥文化传播有限公司、上海泛微网络科技股份有限公司、山东强比信息技术有限公司、武汉类森科技有限公司、善行网页设计公司、深圳飞思安诺网络技术有限公司、中国城乡统筹科学发展办公室、雷风影视、中国新闻传媒网、百度智能云、中国文化产业协会、春哥技术博客团队、帝国软件、Sumpple、ThinkCMF、Indexhibit、Xnview、SemCms 和 Guojiz。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、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、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。北京铭图天成信息技术有限公司、长春嘉诚信息技术股份有限公司、南京众智维信息科技有限公司、山东云天安全技术有限公司、国瑞数码零点实验室、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、浙江国利网安科技有限公司、北京君信安科技有限公司、广州锦行网络科技有限公司、北京圣博润高新技术股份有限公司、内蒙古奥创科技有限公司、河南信安世纪科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京智游网安科技有限公司、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 2794 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 1995 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）	845	845
阿里云计算有限公司	812	0
斗象科技（漏洞盒子）	635	635
上海交大	515	515
哈尔滨安天科技集团股份有限公司	234	0
北京天融信网络安全技术有限公司	135	1
华为技术有限公司	117	0
北京神州绿盟科技有限公司	108	7
四川无声信息技术有限公司	103	103
深信服科技股份有限公司	82	0
新华三技术有限公司	48	0
厦门服云信息科技有限公司	47	1
北京启明星辰信息安全技术有限公司	47	0
恒安嘉新(北京)科技股份公司	27	0
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	2	0
沈阳东软系统集成工程有限公司	2	2
北京铭图天成信息技术有限公司	163	163
长春嘉诚信息技术股份有限公司	93	93
南京众智维信息科技有限公司	64	64
山东云天安全技术有限公司	44	44
国瑞数码零点实验室	30	30

山东新潮信息技术有限公司	30	30
任子行网络技术股份有限公司	19	19
浙江国利网安科技有限公司	12	12
北京君信安科技有限公司	9	9
广州锦行网络科技有限公司	9	9
北京圣博润高新技术股份有限公司	6	6
内蒙古奥创科技有限公司	5	5
河南信安世纪科技有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京智游网安科技有限公司	2	2
上海市信息安全测评认证中心	2	2
CNCERT 天津分中心	15	15
CNCERT 甘肃分中心	10	10
CNCERT 黑龙江分中心	2	2
CNCERT 浙江分中心	2	2
个人	162	162
报送总计	4463	2794

本周漏洞按类型和厂商统计

本周，CNVD 收录了 405 个漏洞。应用程序 234 个，WEB 应用 103 个，操作系统 50 个，网络设备（交换机、路由器等网络端设备）10 个，数据库 5 个，安全产品 2 个，智能设备（物联网终端设备）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	234

WEB 应用	103
操作系统	50
网络设备（交换机、路由器等网络端设备）	10
数据库	5
安全产品	2
智能设备（物联网终端设备）漏洞	1

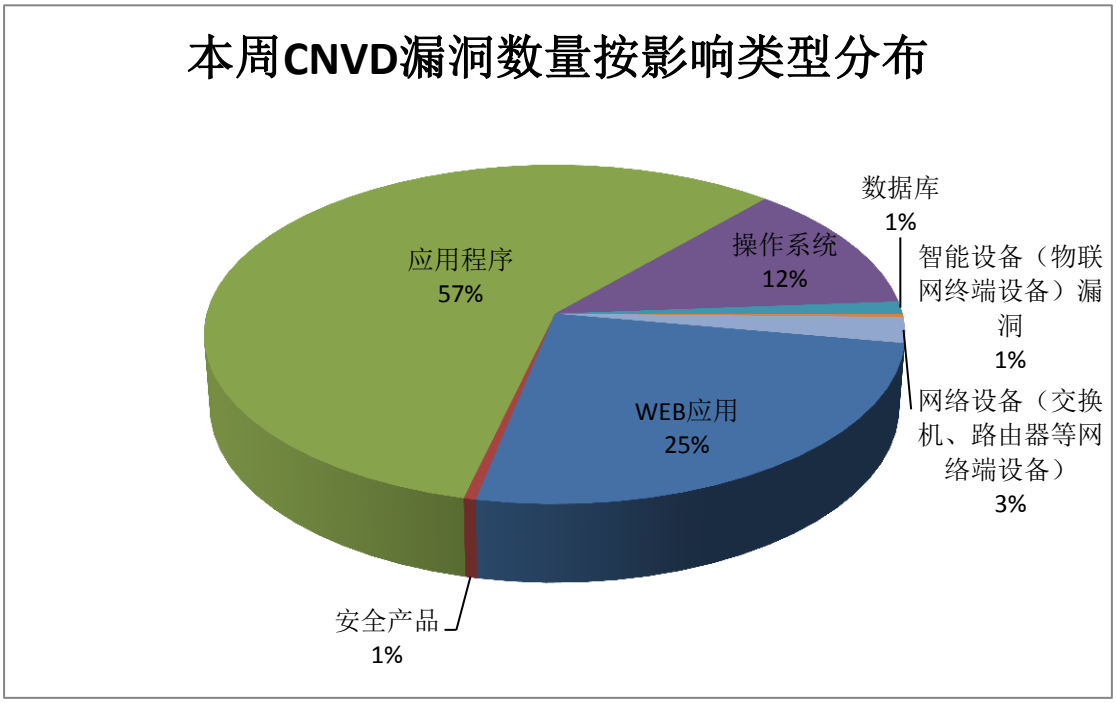

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Linux、IBM 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	90	22%
2	Linux	39	10%
3	IBM	32	8%
4	Google	24	6%
5	Microsoft	19	5%
6	F5	18	4%
7	Advantech	17	4%
8	Atlassian	15	4%
9	Adobe	11	3%
10	其他	140	34%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，3 个移动互联网行业漏洞，29 个工控行业漏洞（如下图所示）。其中，“Cisco NX-OS Software Cisco Fabric Services 组件输入验证错误漏洞、3S-Smart Software Solutions CODESYS Development System 跨站脚本漏洞、Siemens SIMATIC TDC CP51M1 输入验证错误漏洞、Advantech WebAccess 代码注入漏洞”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/

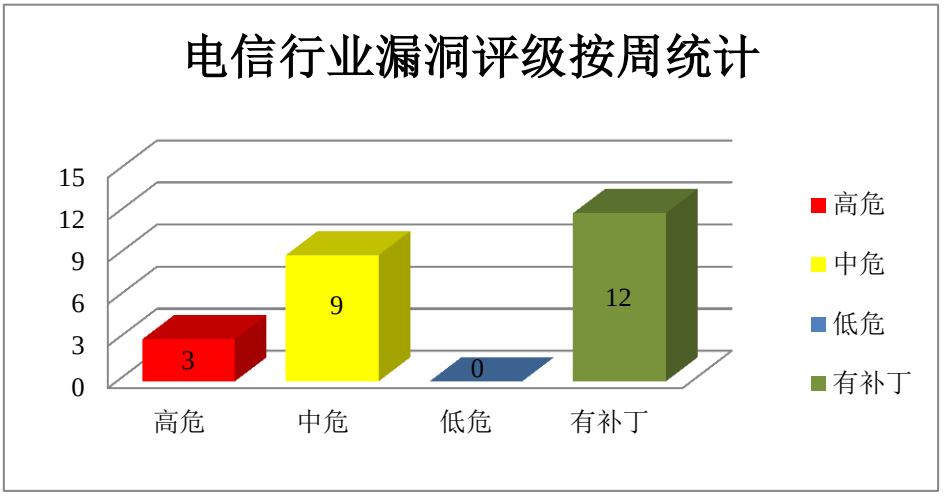

图 3 电信行业漏洞统计

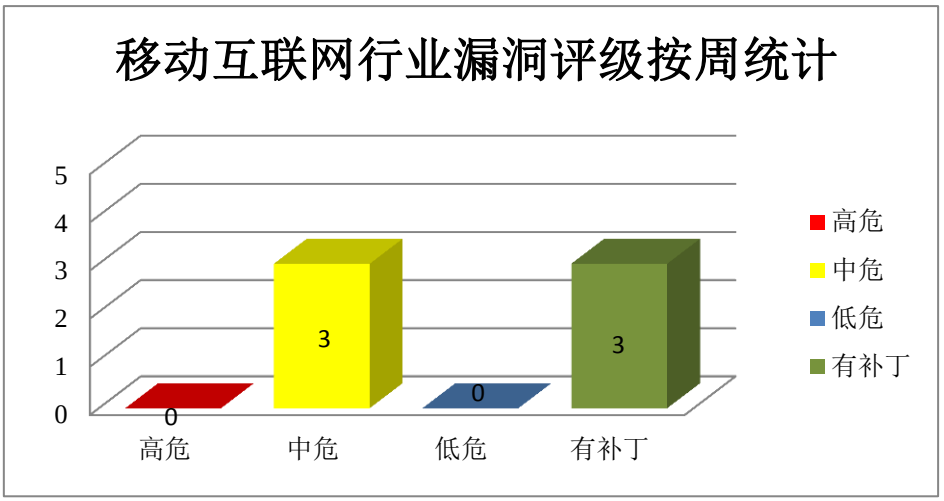

图 4 移动互联网行业漏洞统计

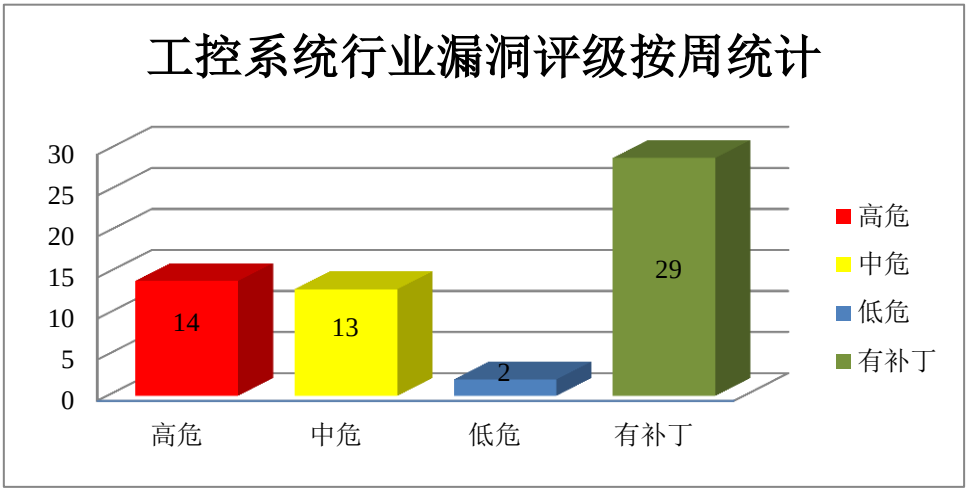

图 5 工控系统行业漏洞统计

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 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。本周，该产品被披露存在远程代码执行和提权漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Compatibility Appraiser 提权漏洞、Microsoft Windows 和 Microsoft Windows Server 提权漏洞（CNVD-2019-31845、CNVD-2019-31847、CNVD-2019-31851、CNVD-2019-31848）、Microsoft Windows Common Log File System Driver 提权漏洞、Microsoft Windows Remote Desktop Client 远程代码执行漏洞、Microsoft Windows Winlogon 提权漏洞。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-2019-31844

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31845

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31847

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31851

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31848

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31850

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31859

http://www.cnvd.org.cn/flaw/show/CNVD-2019-31856

2、Advantech 产品安全漏洞

Advantech WebAccess/SCADA 是一套基于浏览器架构的 SCADA 软件。本周，上述

产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证，上传恶意数据，执行远程代码或导致系统崩溃。

CNVD 收录的相关漏洞包括：Advantech WebAccess/SCADA 缓冲区溢出漏洞（CNVD-2019-32464、CNVD-2019-32466、CNVD-2019-32472、CNVD-2019-32478）、Advantech WebAccess 代码注入漏洞、Advantech WebAccess 代码问题漏洞、Advantech WebAccess/SCADA 任意代码执行漏洞、Advantech WebAccess/SCADA 授权问题漏洞。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-2019-32464
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32466
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32467
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32472
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32474
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32473
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32478
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32479

3、IBM 产品安全漏洞

IBM Spectrum Protect（前称 Tivoli Storage Manager）是一套数据保护平台。IBM Emptoris Sourcing 是一套基于 Web 的企业采购流程管理解决方案。IBM Cognos Controller 是一套商业智能与计划解决方案。IBM Sterling File Gateway 是一套文件传输软件。IBM DB2 是一套关系型数据库管理系统。IBM Jazz for Service Management 是一款提供对服务管理环境可见性的集成服务管理产品。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、添加、修改或删除后端数据库中的信息，导致拒绝服务（服务器崩溃）等。

CNVD 收录的相关漏洞包括：IBM Spectrum Protect 信息泄露漏洞（CNVD-2019-32054）、IBM Spectrum Protect Plus 信息泄露漏洞、IBM Emptoris Sourcing 信息泄露漏洞（CNVD-2019-32434）、IBM Cognos Controller 信息泄露漏洞（CNVD-2019-32435、CNVD-2019-32437）、IBM Sterling File Gateway SQL 注入漏洞、IBM DB2 拒绝服务漏洞（CNVD-2019-32450）、IBM Jazz for Service Management 信息泄露漏洞（CNVD-2019-32453）。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-2019-32054
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32057
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32434
http://www.cnvd.org.cn/flaw/show/CNVD-2019-32435

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32437

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32446

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32450

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32453

4、F5 产品安全漏洞

F5 BIG-IP 是一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。F5 BIG-IP APM 是一套访问和安全解决方案。APM Client 是一套 APM 客户端软件。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敏感信息，执行客户端代码，导致服务中断等。

CNVD 收录的相关漏洞包括：F5 BIG-IP 输入验证错误漏洞（CNVD-2019-32029、CNVD-2019-32030）、F5 BIG-IP Application Security Manager 资源管理错误漏洞、F5 BIG-IP 拒绝服务漏洞（CNVD-2019-32035）、F5 BIG-IP 信任管理问题漏洞、F5 BIG-IP 跨站脚本漏洞（CNVD-2019-32037）、F5 BIG-IP PEM 输入验证错误漏洞、F5 BIG-IP APM 和 BIG-IP APM Clients svpn 权限提升漏洞。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-2019-32029

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32030

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32031

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32035

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32036

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32037

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32038

http://www.cnvd.org.cn/flaw/show/CNVD-2019-32042

5、ZOHO ManageEngine Application Manager SQL 注入漏洞

ZOHO ManageEngine Application Manager 是一套应用程序监控管理系统。本周，ZOHO ManageEngine Application Manager 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行非法 SQL 命令。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-2019-32071

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-2019-31387	Siemens SIMATIC TDC CP51M1 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://support.industry.siemens.com/cs/document/27049282/firmware-updates-for-simatic-tdc-cp51m1?dti=0&lc=en-AZ
CNVD-2019-31643	Linux kernel 空指针解引用漏洞（CNVD-2019-31643）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lkml.org/lkml/2019/9/9/487
CNVD-2019-31842	Jenkins Git client 插件命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/jenkinsci/git-client-plugin
CNVD-2019-32011	Google Chrome Media 资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html
CNVD-2019-32060	Cisco NX-OS Software Cisco Fabric Services 组件输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-fsip-dos
CNVD-2019-32064	Cisco NX-OS Software 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-nxos-ntp-dos
CNVD-2019-32079	Aspose.PDF for C++资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.aspose.com
CNVD-2019-32230	Delta Electronics TPEditor 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：http://www.deltaww.com/services/DownloadCenter2.aspx?secID=8&pid=2&tid=0&CID=06&itemID=060302&typeID=1&downloadID=&title=&dataType=8;&check=1&hl=en-US
CNVD-2019-32334	uriparser 整数溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/uriparser/uriparser/blob/uriparser-0.9.0/ChangeLog
CNVD-2019-32462	3S-Smart Software Solutions CODESYS V3 web server 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://www.codesys.com/

小结：本周，Microsoft 产品被披露存在远程代码执行和提权漏洞，攻击者可利用漏

洞提升权限，执行任意代码。此外，Advantech、IBM、F5 等多款产品被披露存在多个漏洞，攻击者可利用漏洞查看、添加、修改或删除后端数据库中的信息，绕过身份验证，上传恶意数据，执行远程代码或导致系统崩溃等。另外，ZOHO ManageEngine Application Manager 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行非法 SQL 命令。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、FlameCMS login.php 文件 SQL 注入漏洞

验证描述

FlameCMS 是一套基于 PHP 的开源内容管理系统（CMS）。

FlameCMS 3.3.5 版本中的 account/login.php 文件存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令。

验证信息

POC 链接：http://www.iwantacve.cn/index.php/archives/317/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-32198

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. Harbor 任意管理员注册漏洞

Harbor 是一个用于存储和分发 Docker 镜像的企业级 Registry 服务器，通过添加一些企业必需的功能特性，例如安全、标识和管理等，扩展了开源 Docker Distribution。近日 Harbor 曝出一个垂直越权漏洞，因注册模块对参数校验不严格，可导致任意管理员注册。

参考链接：https://www.freebuf.com/vuls/214767.html

2. 比特币钱包 Electrum 遭受黑客钓鱼攻击 至少 1450 枚比特币遭窃

黑客通过恶意服务器向 Electrum 客户端广播消息，提示用户更新至 v4.0.0 版本，如果用户按照提示安装了此“携带后门的客户端”，则私钥会遭到窃取，所有的数字资产将被盗。截至发稿时，伪造 Electrum 升级提示的钓鱼攻击已盗窃至少 1450 枚 BTC（被

盗数量由一名用户、反恶意软件公司 Malwarebytes 和 Electrum 官方统计而来），总价值约 1160 万美元。

参考链接：http://www.techweb.com.cn/blockchain/2019-09-19/2755206.shtml

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