国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 06 月 17 日-2019 年 06 月 23 日 **2019 年第 25 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 200 个，其中高危漏洞 50 个、中危漏洞 99 个、低危漏洞 51 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 73 个（占 37%），其中互联网上出现“RedwoodHQ 绕过身份验证漏洞、Open Faculty Evaluation System 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 1736 个，与上周（2883 个）环比下降 40%。

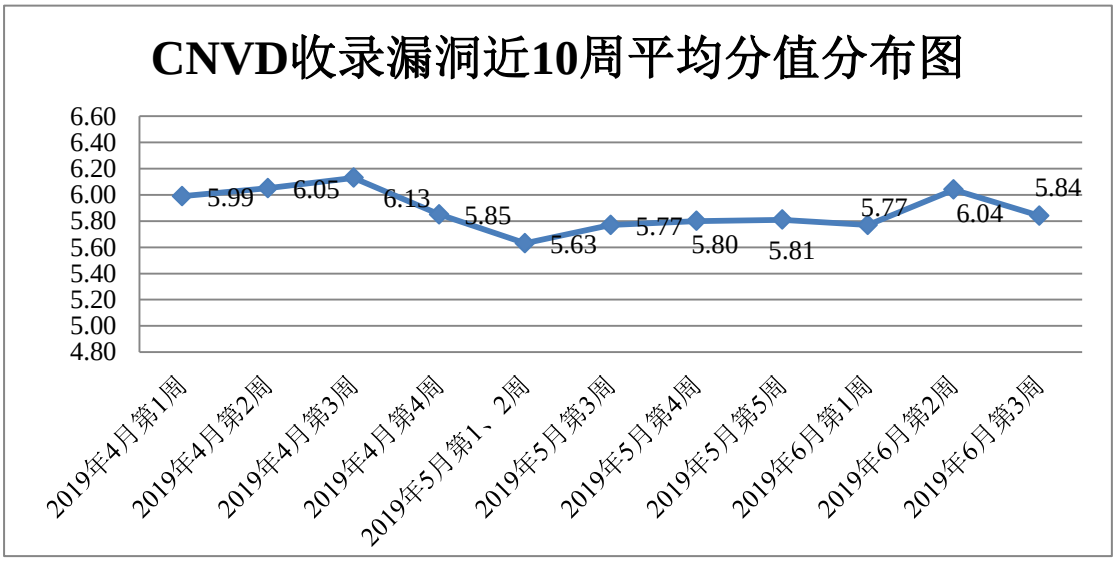

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 50 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 275 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 76 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38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：

浙江齐治科技股份有限公司、中国邮政速递物流股份有限公司、中银消费金融有限公司、北京电信通电信工程有限公司、微软（中国）有限公司、居易科技股份有限公司、北京亿赛通科技发展有限责任公司、宁波易企网络科技有限公司、上海茸易科技有限公司、中建材集团进出口有限公司、台州精迅信息技术有限公司、北京致远协创软件有限公司、洛阳众智软件科技股份有限公司、河南利梭互联网信息技术有限公司、深圳市锟铻科技有限公司、美图公司、中铁十二局集团铁路养护公司、中铁二十一局集团有限公司、广州力洋网络科技有限公司、中铁十七局集团有限公司、长沙德尚网络科技有限公司、重庆讯迈科技发展有限公司、江苏西格数据科技有限公司、淄博闪灵网络科技有限公司、合肥江湖信息网络科技有限公司、网新科技集团有限公司、理光(中国)投资有限公司、青岛品赢网络技术有限公司、北京昱新科技有限公司、北京邦永科技有限公司、北京网康科技有限公司、深圳锟铻科技有限公司、珠海信达九州科技有限公司、DM 建站系统、安徽启明星工作室、中国电机工程学会、中国知网、中国农业机械化科学研究院、中国地球物理学会、中国工程科技知识中心、科威工作室、Catfish CMS、Oracle、Adobe、Zzzcms、LaySNS、UQCMS、CSCMS。

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、深信服科技股份有限公司、华为技术有限公司、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。北京铭图天成信息技术有限公司、国瑞数码零点实验室、南京众智维信息科技有限公司、任子行网络技术股份有限公司、上海银基信息安全技术股份有限公司、山石网科通信技术有限公司、北京冠程科技有限公司、江苏天网计算机技术有限公司、内蒙古奥创科技有限公司、广州锦行网络科技有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、四川无国界信息技术有限公司及其他个人白帽子向 CNVD 提交了 1736 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 1358 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）	778	778
奇安信网神（补天平台）	580	580

北京天融信网络安全技术有限公司	204	0
哈尔滨安天科技集团股份有限公司	146	0
深信服科技股份有限公司	88	0
华为技术有限公司	73	0
北京数字观星科技有限公司	62	0
新华三技术有限公司	54	0
恒安嘉新(北京)科技股份公司	39	0
中新网络信息安全股份有限公司	16	16
厦门服云信息科技有限公司	10	0
北京神州绿盟科技有限公司	5	5
南京联成科技发展股份有限公司	3	3
北京知道创宇信息技术股份有限公司	1	0
北京启明星辰信息安全技术有限公司	1	1
北京铭图天成信息技术有限公司	43	43
国瑞数码零点实验室	43	43
南京众智维信息科技有限公司	28	28
任子行网络技术股份有限公司	25	25
上海银基信息安全技术股份有限公司	20	20
山石网科通信技术有限公司	8	8
北京冠程科技有限公司	4	4
江苏天网计算机技术有限公司	4	4
内蒙古奥创科技有限公司	3	3

广州锦行网络科技有限公司	3	3
山东云天安全技术有限公司	2	2
河南信安世纪科技有限公司	1	1
四川无国界信息技术有限公司	1	1
CNCERT 西藏分中心	11	11
CNCERT 海南分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 青海分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 浙江分中心	1	1
个人	150	150
报送总计	2413	1736

本周漏洞按类型和厂商统计

本周，CNVD 收录了 200 个漏洞。应用程序 102 个，WEB 应用 58 个，网络设备（交换机、路由器等网络端设备）29 个，操作系统 9 个，安全产品 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	102
WEB 应用	58
网络设备（交换机、路由器等网络端设备）	29
操作系统	9
安全产品	2

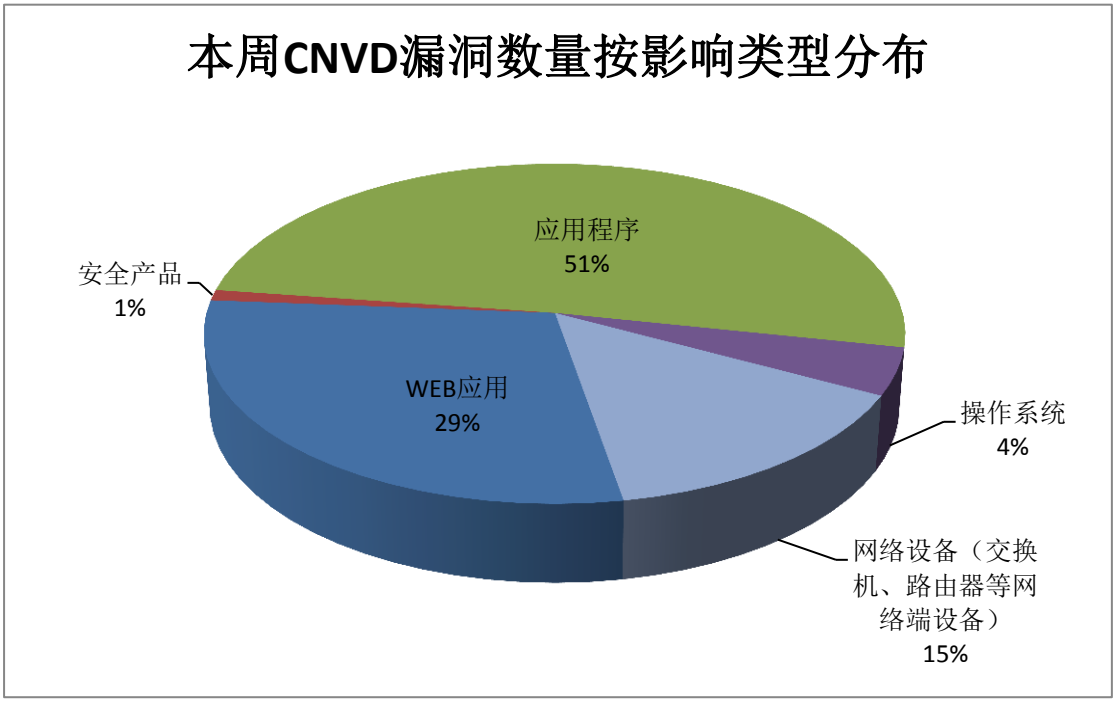

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、深圳搜豹网络有限公司、Cisco 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	IBM	14	7%
2	深圳搜豹网络有限公司	13	7%
3	Cisco	12	6%
4	Adobe	9	5%
5	Qualcomm	9	5%
6	Microsoft	8	4%
7	Nextcloud	7	4%
8	Securifi	7	4%
9	Wireshark	7	4%
10	其他	114	57%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，2 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，“FreePBX Backup 模块命令注入漏洞、Cisco RV110W、R

V130W、RV215W 管理界面拒绝服务漏洞、Securifi Almond 命令注入漏洞、Advantech WebAccess/SCADA 缓冲区溢出漏洞（ CNVD-2019-18756）、Teltonika RUT9XX OS 命令注入漏洞”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/

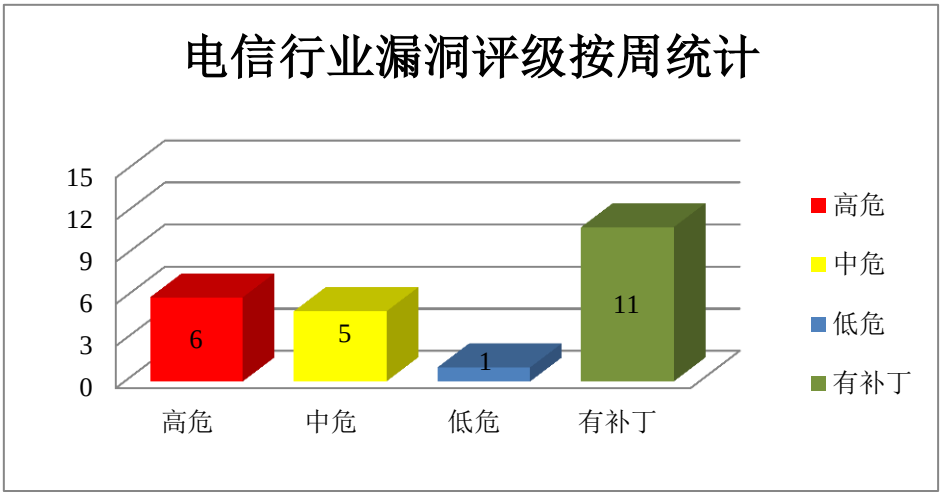

图 3 电信行业漏洞统计

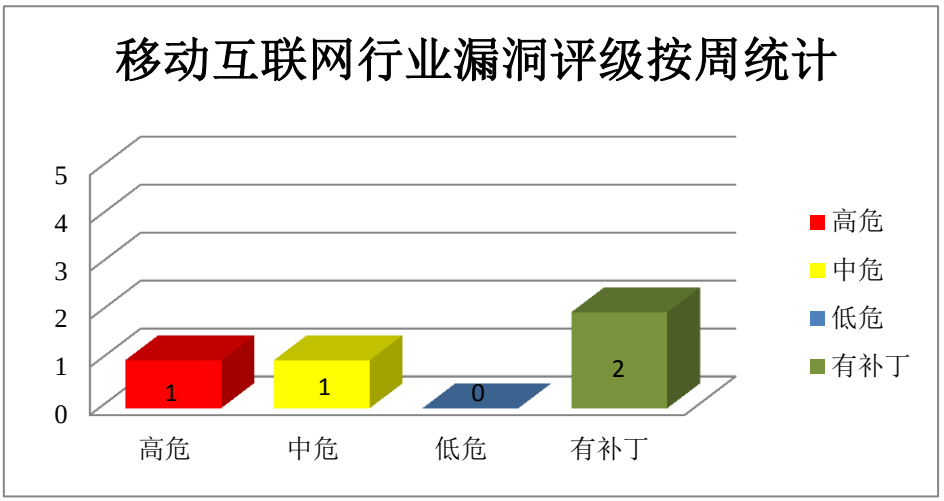

图 4 移动互联网行业漏洞统计

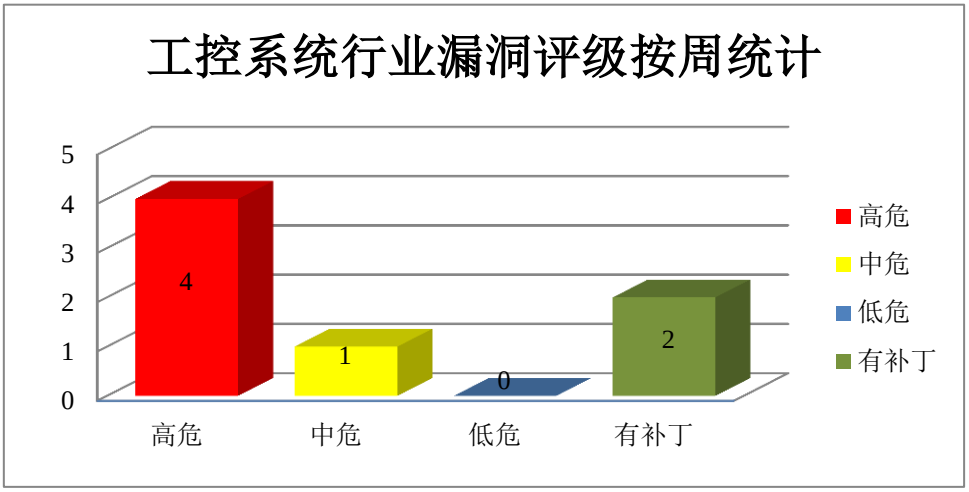

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM API Connect（APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM WebSphere Application Server Network Deployment 是 IBM 的集成软件平台。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Marketing Platform 是一套营销平台。IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。IBM Cognos Controller 是一套商业智能与计划解决方案。IBM Campaign（前称 Unica Campaign）是一套用于帮助营销人员设计、执行、衡量和优化营销广告的管理解决方案。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，执行任意命令。

CNVD 收录的相关漏洞包括：IBM API Connect 信息泄露漏洞（CNVD-2019-18508）、IBM WebSphere Application Server ND 远程代码执行漏洞、IBM Maximo Asset Management CSV 注入漏洞、IBM Marketing Platform 信息泄露漏洞、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2019-18838）、IBM Cognos Controller 信息泄露漏洞（CNVD-2019-18843）、IBM Maximo Asset Management 信息泄露漏洞（CNVD-2019-18848）、IBM Campaign 任意下载漏洞。其中，“IBM WebSphere Application Server ND 远程代码执行漏洞、IBM Maximo Asset Management CSV 注入漏洞”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-2019-18508

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18510

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18726

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18731

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18838

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18843

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18848

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18849

2、Cisco 产品安全漏洞

Cisco Video Surveillance Manager 是一款视频监控管理器。Cisco RV110W 是一款 Wireless-N VPN 防火墙路由器。Cisco RV130W 是一款 Wireless-N 多功能 VPN 路由器 Cisco RV215W 是一款 Wireless-N VPN 路由器。Cisco Integrated Management Controller（IMC）是一套用于对 UCS（统一计算系统）进行管理的软件。Cisco Prime Service Catalog（PSC）是一套通过单一的门户网站提供所有 IT 服务的服务目录解决方案。Cisco Meeting Server 是视频会议解决方案 Cisco Email Security Appliance（ESA）是一个电子邮件安全设备。Cisco Security Manager（CSM）是一套企业级的管理应用。Cisco StarOS 是一套路由器操作系统，可控制整个系统逻辑，可控制进程和 CLI。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，以 root 权限执行任意的命令,造成拒绝服务（消耗可用资源）。

CNVD 收录的相关漏洞包括：Cisco Video Surveillance Manager 信息泄露漏洞、Cisco RV110W、RV130W、RV215W 管理界面拒绝服务漏洞、Cisco Integrated Management Controller 操作系统命令注入漏洞、Cisco Prime Service Catalog 跨站请求伪造漏洞（CNVD-2019-18752）、Cisco Meeting Server CLI 命令注入漏洞、Cisco Email Security Appliance AsyncOS Software 远程安全绕过漏洞、Cisco Security Manager XML 外部实体注入漏洞、Cisco StarOS 拒绝服务漏洞。其中，“Cisco RV110W、RV130W、RV215W 管理界面拒绝服务漏洞、Cisco Prime Service Catalog 跨站请求伪造漏洞（CNVD-2019-18752）、Cisco StarOS 拒绝服务漏洞”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-2019-18483

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18734

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18750

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18752

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18855

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18857

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18858

http://www.cnvd.org.cn/flaw/show/CNVD-2019-18860

3、Adobe 产品安全漏洞

Adobe Campaign Classic（ACC）是一套跨渠道客户体验营销平台。Adobe ColdFusion 是一套快速应用程序开发平台。Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 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敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Campaign Classic 信息泄露漏洞（CNVD-2019-18621、CNVD-2019-18623）、Adobe Campaign Classic 命令注入漏洞、Adobe ColdFusion 安全绕过漏洞（CNVD-2019-18625）、Adobe ColdFusion 命令注入漏洞、Adobe Acrobat/Reader 内存错误引用漏洞（CNVD-2019-18853、CNVD-2019-18852、CNVD-2019-18854）。其中，除“Adobe Campaign Classic 信息泄露漏洞（CNVD-2019-18621、CNVD-2019-18623）”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-2019-18621
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18623
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18622
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18625
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18626
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18853
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18852
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18854

4、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。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。ChakraCore 是使用在 Edge 浏览器中的一个开源的 ChakraJavaScript 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft Windows IIS Server 拒绝服务漏洞、Microsoft Edge 安全功能绕过漏洞（CNVD-2019-18613）、Microsoft Windows Event Viewer 信息泄露漏洞、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-18615）、Microsoft Windows 拒绝服务漏洞（CNVD-2019-18614）、Microsoft Edge 和 ChakraCore 缓冲区溢出漏洞（CNVD-2019-18617）、Microsoft Internet Explorer 和 Edge 信息泄露漏洞（CNVD-2019-18616）、Microsoft Internet Explorer 和 Edge 脚本引擎远程内存破坏漏洞。其中，“Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-18615）、Microsoft Edge 和 ChakraCore 缓冲区溢出漏洞（CNVD-2019-18617）、Microsoft Internet Explorer 和 Edge 脚本引擎远程内存破坏漏洞”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-2019-18611
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18613
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18612
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18615
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18614
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18617
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18616
http://www.cnvd.org.cn/flaw/show/CNVD-2019-18851

5、Teltonika RUT950 拒绝服务漏洞

Teltonika RUT950 是一款 LET 路由器产品。Teltonika RUT950 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒接服务（占用内存及可用空间）。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-2019-18738

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-2019-18492	REDAXO SQL 注入漏洞（CNVD-2019-18492）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/redaxo/redaxo/releases/tag/5.6.3
CNVD-2019-18494	Teltonika RUT9XX OS 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://teltonika.lt/product/rut955/
CNVD-2019-18496	Teltonika RUT9XX 任意命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://teltonika.lt/product/rut955/
CNVD-2019-18507	Wireshark 内存泄漏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=6e920ddc3cad2886ef07ca1a8e50e2a5c50986f7
CNVD-2019-18610	Mozilla Firefox 和 Mozilla Firefox ESR 类型混淆漏洞	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.mozilla.org/en-US/security/advisories/mfsa2019-18/

CNVD-2019-18743	Securifi Almond 缓冲区溢出漏洞（CNVD-2019-18743）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.securifi.com/
CNVD-2019-18753	Cisco SD-WAN Solution 权限许可和访问控制问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190619-sdwan-privilescal
CNVD-2019-18756	Advantech WebAccess/SCADA 缓冲区溢出漏洞（ CNVD-2019-18756）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.advantech.com/
CNVD-2019-18839	Advantech WebAccess/SCADA 缓冲区溢出漏洞（ CNVD-2019-18839）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.advantech.com/
CNVD-2019-18841	Linux kernel 资源管理错误漏洞（CNVD-2019-18841）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.kernel.org/

小结：本周，IBM 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意命令。此外，Cisco、Adobe、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，以 root 权限执行任意的命令，造成拒绝服务等。Teltonika RUT950 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒接服务（占用内存及可用空间）。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、RedwoodHQ 绕过身份验证漏洞

验证描述

RedwoodHQ 是一款开源的自动化测试框架。该产品支持 Java、Groovy、Python 和 C#等编程语言，能够创建可读的关键字驱动的测试用例。

RedwoodHQ 2.5.5 版本中存在安全漏洞。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。允许远程攻击者通过 con.automationFramework 用户插入一个调用来创建管理用户。

验证信息

POC 链接：https://www.exploit-db.com/exploits/46992

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-18870

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. 戴尔预装软件曝出安全漏洞

数百万台戴尔电脑预装的软件 SupportAssist 曝出了一个严重的安全漏洞，漏洞细节没有披露，只是表示远程攻击者可以利用该漏洞完全控制受影响的机器。SupportAssist 由 PC Doctor 开发，用于主动监视机器，自动检测故障并通报戴尔。受影响的版本是 Dell SupportAssist for Business PCs version 2.0 和 Dell SupportAssist for Home PCs version 3.2.1 以及所有旧版本，戴尔建议客户尽可能快的更新到新版本 v2.0.1 或 v3.2.2。

参考链接：https://www.solidot.org/story?sid=61087

2. TP-LINK Wi-Fi 中继器出现漏洞，可用于远程代码执行

近日，一些 TP-Link 的 Wi-Fi 中继器设备存在严重的远程代码执行漏洞，漏洞可导致外来攻击者获取设备权限并执行任意命令。攻击者还可以通过在设备连接的操作系统上执行任意的 shell 命令来进行恶意行为。黑客可以通过这个漏洞向所在系统进行横向提权，直到获得管理员权限。

参考链接：https://www.freebuf.com/news/206346.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