国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 05 月 27 日-2019 年 06 月 03 日 **2019 年第 22 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 293 个，其中高危漏洞 97 个、中危漏洞 167 个、低危漏洞 29 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 134 个（占 46%），其中互联网上出现“Joomla Com_Attachments 组件文件上传漏洞、VFront 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 1605 个，与上周（2475 个）环比下降 35%。

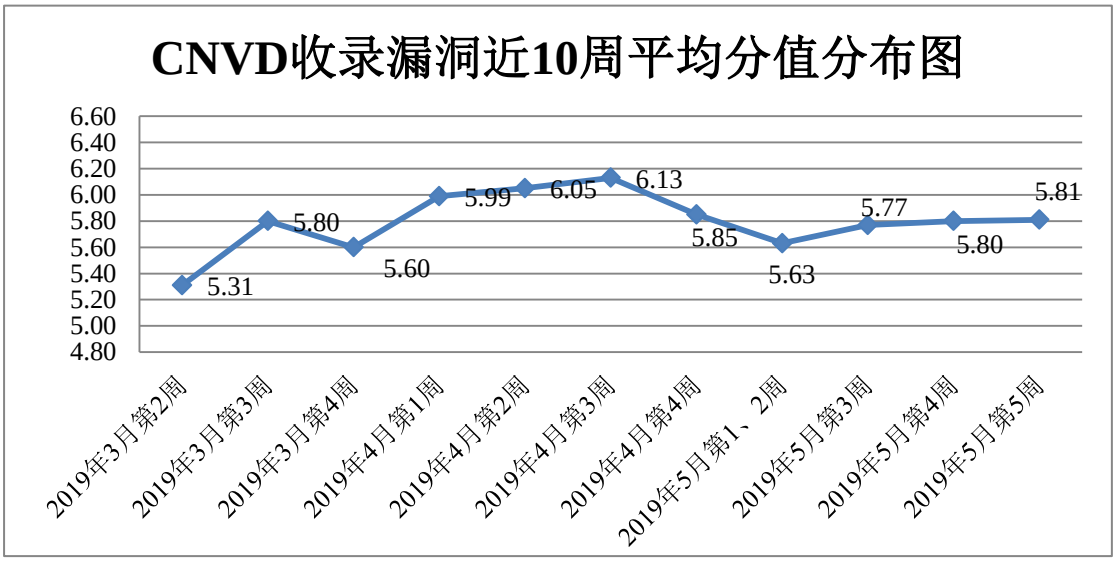

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 513 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 25 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：

上海安达通信息安全技术股份有限公司、厦门维品网络科技有限公司、西安凤巢网络科技有限公司、中铁二十一局集团有限公司、厦门得推网络科技有限公司、杭州可道云网络有限公司、北京谋智火狐信息技术有限公司、上海亿速网络科技有限公司、深圳搜豹网络有限公司、微软(中国)有限公司、沧州市凡诺广告传媒有限公司、抚顺市经纬网络技术开发有限公司、北京辅仁心智软件科技有限公司、浙江齐治科技有限公司、屏通科技股份有限公司、哈尔滨伟成科技有限公司、苏州天宫信息技术有限公司、中国科学院软件研究所、中国标准化研究院、中国金属科学与装备制造技术信息网、中国肉类协会会展交流网、米酷资源网、中国电子电路行业协会、CAMDS 管理委员会秘书处、施耐德、米酷资源网、中环工作室、华夏信财、信呼、熊海 CMS、WMCMS 团队、世界卫生组织、欧盟委员会、世界气象组织、中国种养殖网、vaeThink、slideshow、numexpr、zzzcms、Anaconda、sqlalchemy、tjpcms、ZZCMS、Bo-Blog、FATEK、FastAdmin。

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、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、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。任子行网络技术股份有限公司、国瑞数码零点实验室、山东云天安全技术有限公司、南京众智维信息科技有限公司、内蒙古奥创科技有限公司、北京铭图天成信息技术有限公司、北京圣博润高新技术股份有限公司、长春嘉诚信息技术股份有限公司、四川无国界信息技术有限公司、江苏安又恒信息科技有限公司、山石网科通信技术股份有限公司、上海银基信息安全技术股份有限公司、河南信安世纪科技有限公司、山东华鲁科技发展股份有限公司、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 1605 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 1066 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）	598	598
奇安信网神（补天平台）	468	468
北京天融信网络安全技术有限公司	392	3

深信服科技股份有限公司	107	0
华为技术有限公司	103	0
北京数字观星科技有限公司	61	0
北京启明星辰信息安全技术有限公司	53	0
四川无声信息技术有限公司	37	37
新华三技术有限公司	34	0
哈尔滨安天科技集团股份有限公司	32	0
北京神州绿盟科技有限公司	27	2
北京知道创宇信息技术股份有限公司	26	22
中新网络信息安全股份有限公司	22	22
恒安嘉新(北京)科技股份公司	13	0
厦门服云信息科技有限公司	5	1
西安四叶草信息技术有限公司	5	5
南京联成科技发展股份有限公司	2	2
厦门服云信息科技有限公司	1	1
任子行网络技术股份有限公司	95	95
国瑞数码零点实验室	75	75
山东云天安全技术有限公司	60	60
南京众智维信息科技有限公司	44	44
内蒙古奥创科技有限公司	42	42
北京铭图天成信息技术有限公司	12	12
北京圣博润高新技术股份有限公司	12	12

长春嘉诚信息技术股份有限公司	11	11
四川无国界信息技术有限公司	8	8
江苏安又恒信息科技有限公司	3	3
山石网科通信技术股份有限公司	2	2
上海银基信息安全技术股份有限公司	2	2
河南信安世纪科技有限公司	1	1
山东华鲁科技发展股份有限公司	1	1
上海并擎软件科技有限公司	1	1
CNCERT 甘肃分中心	6	6
CNCERT 四川分中心	5	5
CNCERT 湖南分中心	4	4
CNCERT 上海分中心	4	4
CNCERT 河北分中心	2	2
CNCERT 浙江分中心	2	2
CNCERT 西藏分中心	1	1
个人	188	188
报送总计	2430	1605

本周漏洞按类型和厂商统计

本周，CNVD 收录了 293 个漏洞。应用程序 157 个，WEB 应用 77 个，操作系统 20 个，网络设备（交换机、路由器等网络端设备）17 个，安全产品 12 个，数据库 5 个，智能设备（物联网终端设备）漏洞 5 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	157
WEB 应用	77

操作系统	20
网络设备（交换机、路由器等网络端设备）	17
安全产品	12
数据库	5
智能设备（物联网终端设备）漏洞	5

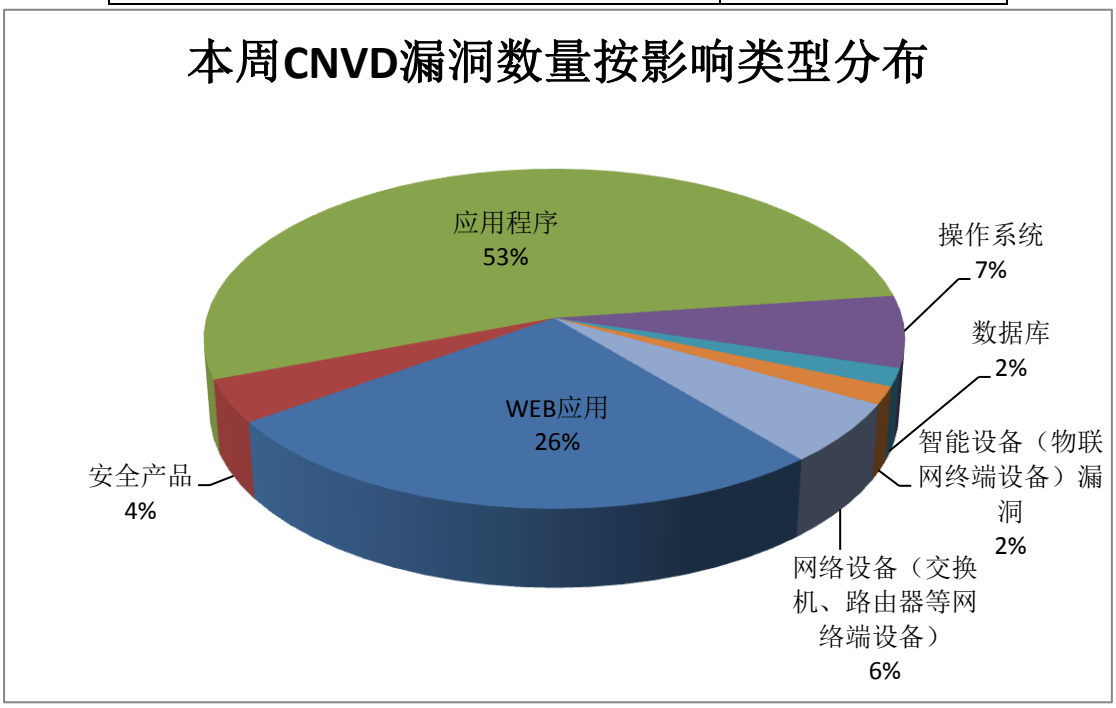

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Schneider Electric、Open-Xchange 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	Microsoft	47	16%
2	Schneider Electric	21	7%
3	Open-Xchange	11	4%
4	WordPress	11	4%
5	爱客 CMS	11	4%
6	Joomla!	10	3%
7	Oracle	8	3%
8	贴心猫(imcat)	6	2%
9	FasterXML	4	1%
10	其他	164	56%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，19 个移动互联网行业漏洞，21 个工控行业漏洞（如下图所示）。其中，“Open-Xchange OX App Suite 访问控制错误漏洞、ISC BIND 拒绝服务漏洞（CNVD-2019-16222）、Open-Xchange OX App Suite 授权问题漏洞、Citrix Systems Workspace App 访问控制错误漏洞”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/

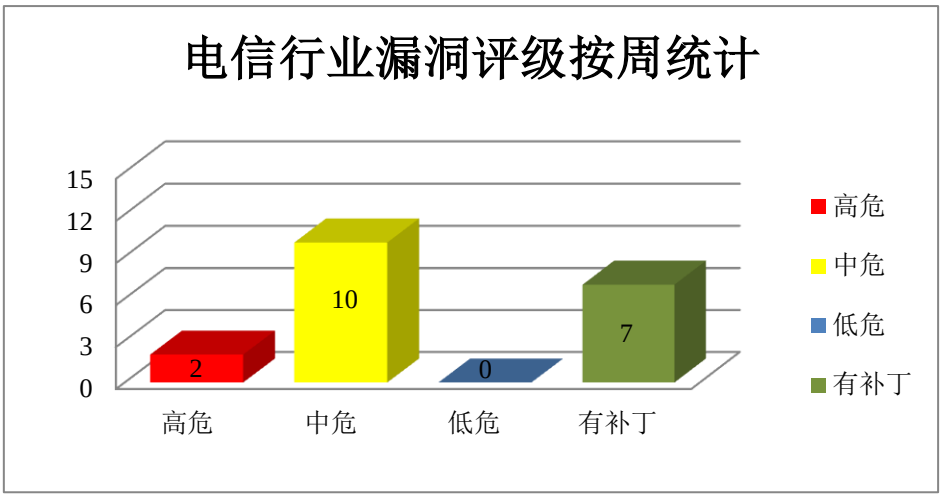

图 3 电信行业漏洞统计

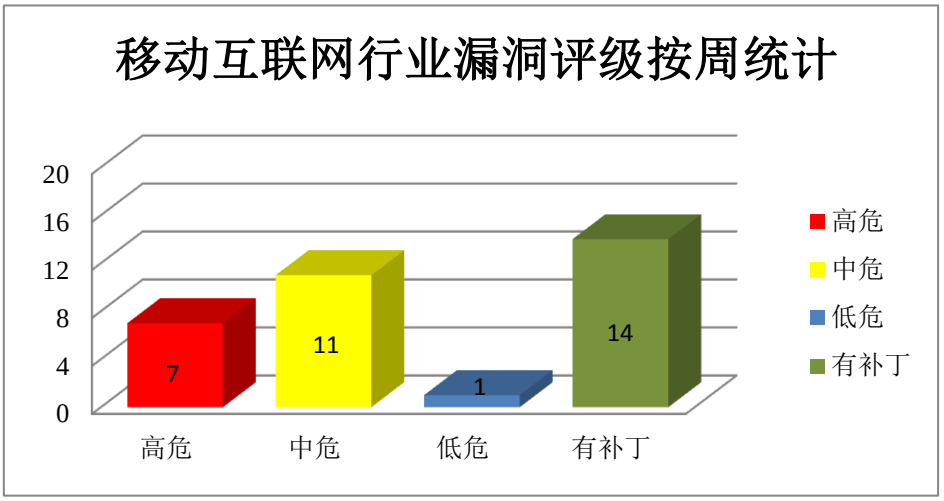

图 4 移动互联网行业漏洞统计

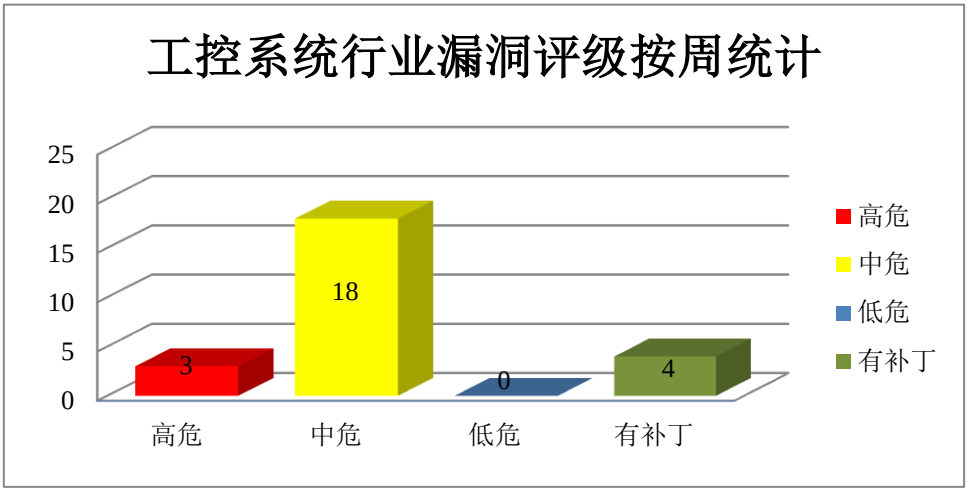

图 5 工控系统行业漏洞统计

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 Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft 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。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Microsoft Edge 和 ChakraCore 缓冲区溢出漏洞（CNVD-2019-16202、CNVD-2019-16201、CNVD-2019-16203、CNVD-2019-16206、CNVD-2019-16205、CNVD-2019-16207）、Microsoft Internet Explorer 缓冲区溢出漏洞（CNVD-2019-16204）、Microsoft Edge 缓冲区溢出漏洞。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-2019-16202

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16201

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16203

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16204

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16206

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16205

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16207

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16208

2、Schneider Electric 产品安全漏洞

Schneider Electric Modicon M580、M340 是一款可编程自动化控制器。Schneider Electric Triconex TriStation Emulator 是一款 Triconex 仿真模拟器。Schneider Electric 1st Gen Pelco Sarix Enhanced Camera 是一系列固定式 IP 摄像机。Schneider Electric Spectra Enhanced PTZ Camera 是一系列球型 IP 摄像机。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，可进行拒绝服务攻击，执行任意的操作系统命令等。

CNVD 收录的相关漏洞包括：Schneider Electric Modicon 越界写拒绝服务漏洞、Schneider Electric Modicon 非法内存块写拒绝服务漏洞、Schneider Electric Modicon 非法断点参数拒绝服务漏洞、Schneider Electric Triconex TriStation Emulator 拒绝服务漏洞、Schneider Electric 1st Gen. Pelco Sarix Enhanced Camera 和 Spectra Enhanced PTZ Camera 跨站请求伪造漏洞、Schneider Electric 1st Gen Pelco Sarix Enhanced Camera 命令注入漏洞（CNVD-2019-16261、CNVD-2019-16259）、Schneider Electric 1st Gen. Pelco Sarix Enhanced Camera 和 Spectra Enhanced PTZ Camera 任意 OS 命令执行漏洞。其中，“Schneider Electric 1st Gen Pelco Sarix Enhanced Camera 命令注入漏洞（CNVD-2019-16259）、Schneider Electric 1st Gen. Pelco Sarix Enhanced Camera 和 Spectra Enhanced PTZ Camera 任意 OS 命令执行漏洞”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-2019-15736

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15735

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15745

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15890

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16259

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16262

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16261

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16263

3、Open-Xchange 产品安全漏洞

Open-Xchange OX App Suite 是一套 Web 云桌面环境。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受影响组件敏感信息，执行客户端代码等。

CNVD 收录的相关漏洞包括：Open-Xchange OX App Suite 访问控制错误漏洞（CNVD-2019-15534、CNVD-2019-15677）、Open-Xchange OX App Suite 跨站脚本漏洞（CNVD-2019-15656、CNVD-2019-15675）、Open-Xchange GmbH OX App Suite 跨站脚本漏洞、Open-Xchange OX App Suite 访问控制错误漏洞、Open-Xchange OX App Suite 信息泄露漏洞（CNVD-2019-16163）、Open-Xchange OX App Suite 授权问题漏洞。其中，“Open-Xchange OX App Suite 访问控制错误漏洞（CNVD-2019-15534、CNVD-20

19-16065）、Open-Xchange OX App Suite 授权问题漏洞”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-2019-15534

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15656

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15675

http://www.cnvd.org.cn/flaw/show/CNVD-2019-15677

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16066

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16065

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16163

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16166

4、Oracle 产品安全漏洞

Oracle MySQL 是一套开源的关系数据库管理系统。Oracle JD Edwards Products 是一套全面集成的企业资源计划管理软件套件（ERP）。Oracle Retail Applications 是一套零售应用商店解决方案。Oracle Siebel CRM 是一套客户关系管理解决方案。Oracle Enterprise Manager Products Suite 是一套企业内部部署管理平台。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞未授权读取、更新、插入或删除数据，造成拒绝服务，影响数据的保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2019-16231、CNVD-2019-16233、CNVD-2019-16232、CNVD-2019-16234）、Oracle JD Edwards Products JD Edwards EnterpriseOne Tools 访问控制错误漏洞、Oracle Retail Applications Retail Point-of-Service 访问控制错误漏洞、Oracle Siebel CRM Siebel Core-Server BizLogic Script 访问控制错误漏洞、Oracle Enterprise Manager Products Suite Application Testing Suite 访问控制错误漏洞。其中，“Oracle Retail Applications Retail Point-of-Service 访问控制错误漏洞” 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-2019-16231

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16233

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16232

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16234

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16235

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16236

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16238

http://www.cnvd.org.cn/flaw/show/CNVD-2019-16237

5、Westermo DR-260、DR-250 和 MR-260 跨站请求伪造漏洞

Westermo DR-260 是一款 DSL 路由器。Westermo DR-250 是一款 DSL 路由器。Westermo MR-260 是一款 3G 多媒体路由器。

Westermo DR-260、DR-250 和 MR-260 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。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-2019-15901

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-2019-15523	FreeBSD rtld execl 权限提升漏洞	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.freebsd.org/where.html
CNVD-2019-15544	Sensio Labs Symfony Password validator 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/symfony/symfony/commit/878198cefae028386c6dc800ccbf18f2b9cbff3f
CNVD-2019-15551	Citrix Systems Workspace App 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.citrix.com/article/CTX251986
CNVD-2019-15554	Blogifier 设计漏洞	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/blogifierdotnet/Blogifier/commit/3e2ae11f6be8aab82128f223c2916fab5a408be5
CNVD-2019-15673	Fortinet FortiClient 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/psirt/FG-IR-19-060
CNVD-2019-15674	Xiaomi Yeelight Smart AI Speaker 访问控制错误漏洞	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.mi.com/
CNVD-2019-15875	Cisco Adaptive Security Appliance Software 拒绝服务漏洞（CNVD-2019-15875）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.cisco.com/
CNVD-2019-15880	Apple macOS Mojave APFS 组件代码执行漏洞	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/HT209600

CNVD-2019-15985	OneLogin ruby-saml 身份验证绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/onelogin/ruby-saml
CNVD-2019-16058	Artifex MuJS 栈缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/ccxvii/mujs/commit/da632ca08f240590d2dec786722ed08486ce1be6

小结：本周，Microsoft 被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致缓冲区溢出或堆溢出等。此外，Schneider Electric、Open-Xchange、Oracle 等多款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，未授权读取、更新、插入或删除数据，造成拒绝服务，执行客户端代码等。Westermo DR-260、DR-250 和 MR-260 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。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、VFront 跨站脚本漏洞

验证描述

VFront 是一套使用 PHP 和 Javascript 编写的用于 MySQL 或 PostgreSQL 数据库的开源前端管理工具。

Vfront 0.99.5 版本中存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/153104/VFront-0.99.5-Persistent-Cross-Site-Scripting.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-16223

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. 未修复的漏洞将影响所有 Docker 版本

所有版本的 Docker 目前都容易受到“竞态条件”的攻击，这种攻击手段可使攻击者对主机系统上的任何文件都具有读写访问权限，概念验证代码已经发布。该漏洞类似于 CVE-2018-15664，它为黑客提供了一个窗口，可以指定的程序开始对资源进行操作之前修改资源路径，归属于时间检查（TOCTOU）类型的错误。

该漏洞的核心源于 FollowSymlinkInScope 功能，该功能易受 TOCTOU 攻击。该函数的目的是通过将进程视为 Docker 容器组件来以安全的方式解析指定的路径。解释路径的操作不会立即进行，它会“稍微延时后完成”。攻击者可以通过这个时间差修改路径，该路径最终会以 root 权限进行相关操作。

参考链接：https://www.bleepingcomputer.com/news/security/unpatched-flaw-affects-all-docker-versions-exploits-ready/

2. Office 365 出现网络钓鱼

近日，一种新形式的钓鱼活动出现在网络中，攻击者会将钓鱼内容伪装成 Office 365 点警告邮件，并告知用户他们的账户中出现异常数量的文件删除。钓鱼攻击以 Office 365 警告内容的形式出现，声称用户已触发中级威胁警报，并告知用户在其账户中发生了大量文件删除行为，诱使用户点击警告框。如果用户点击警告框并，会进入伪造的登录页面，一旦输入账号密码，就会被钓鱼网站获取并保存。随后，登录页面会刷新并将用户重定向至正常登陆页面，以掩盖钓鱼行为。微软提醒用户，Microsoft 账户和 outlook 账户的登录表单只会来自 microsoft.com、live.com 或 outlook.com。如果发现有任何来自其他 URL 的 Microsoft 登录表单，请不要使用。

参考链接：https://www.bleepingcomputer.com/news/security/phishing-emails-pretend-to-be-office-365-file-deletion-alerts/

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