国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 4 月 23 日-2018 年 4 月 29 日 **2018 年第 17 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 400 个，其中高危漏洞 136 个、中危漏洞 239 个、低危漏洞 25 个。漏洞平均分值为 6.12。本周收录的漏洞中，涉及 0day 漏洞 94 个（占 24%），其中互联网上出现“D-Link DSL-3782 缓冲区溢出漏洞、Allen Bradley Micrologix 1400 Series B FRN 访问控制漏洞（CNVD-2018-08283）”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 564 个，与上周（695 个）环比下降 19%。

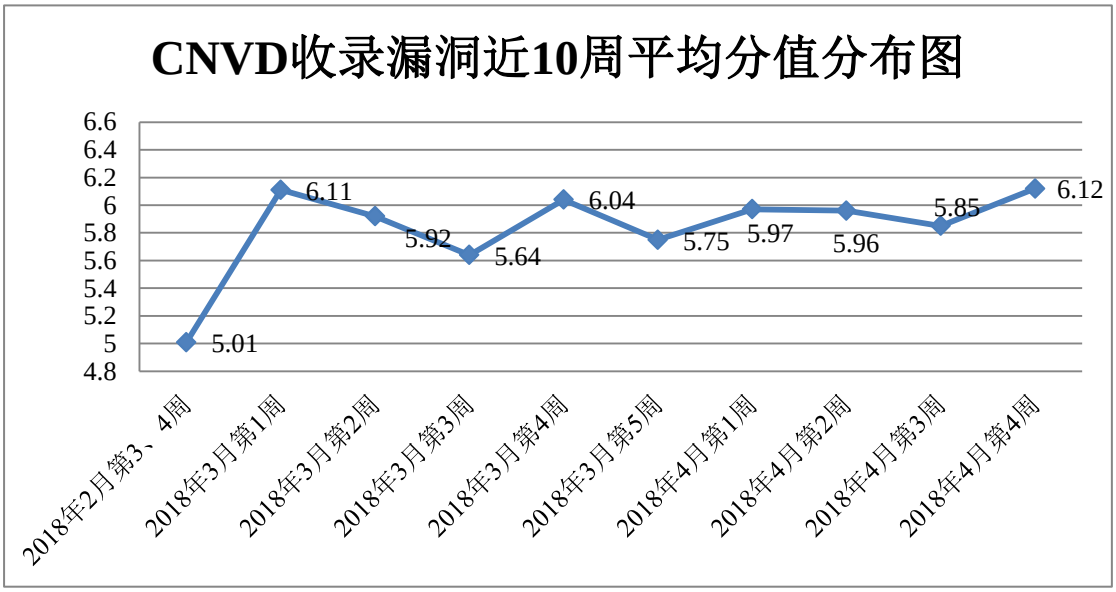

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、哈尔滨安天科技股份有限公司、沈阳东软系统集成工程有限公司、北京神州绿盟科技有限公司、新华

三技术有限公司等单位报送公开收集的漏洞数量较多。山石网科通信技术有限公司、中新网络信息安全股份有限公司、四川虹微技术有限公司（子午攻防实验室）、福建省海峡信息技术有限公司、河北网信智安信息技术有限公司及其他个人白帽子向 CNVD 提交了 564 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）和漏洞盒子向 CNVD 共享的白帽子报送的 377 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
漏洞盒子	283	283
北京天融信网络安全技术有限公司	305	3
哈尔滨安天科技股份有限公司	249	0
沈阳东软系统集成工程有限公司	225	0
北京神州绿盟科技有限公司	161	0
新华三技术有限公司	137	0
华为技术有限公司	98	0
360 网神（补天平台）	94	94
中国电信集团系统集成有限责任公司	79	0
北京数字观星科技有限公司	65	0
恒安嘉新(北京)科技股份公司	47	0
北京无声信息技术有限公司	11	0
北京知道创宇信息技术有限公司	1	0
山石网科通信技术有限公司	22	22
中新网络信息安全股份有限公司	16	16
四川虹微技术有限公司（子午攻防实验室）	11	11
福建省海峡信息技术有限公司	7	7

河北网信智安信息技术有限公司	1	1
CNCERT 山西分中心	15	15
CNCERT 河北分中心	11	11
CNCERT 上海分中心	7	7
CNCERT 天津分中心	4	4
CNCERT 浙江分中心	1	1
CNCERT 广东分中心	1	1
个人	88	88
报送总计	1939	564

本周漏洞按类型和厂商统计

本周，CNVD 收录了 400 个漏洞。其中应用程序漏洞 159 个，WEB 应用漏洞 103 个，操作系统漏洞 62 个，网络设备漏洞 45 个，数据库漏洞 30 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	159
WEB 应用漏洞	103
操作系统漏洞	62
网络设备漏洞	45
数据库漏洞	30
安全产品漏洞	1

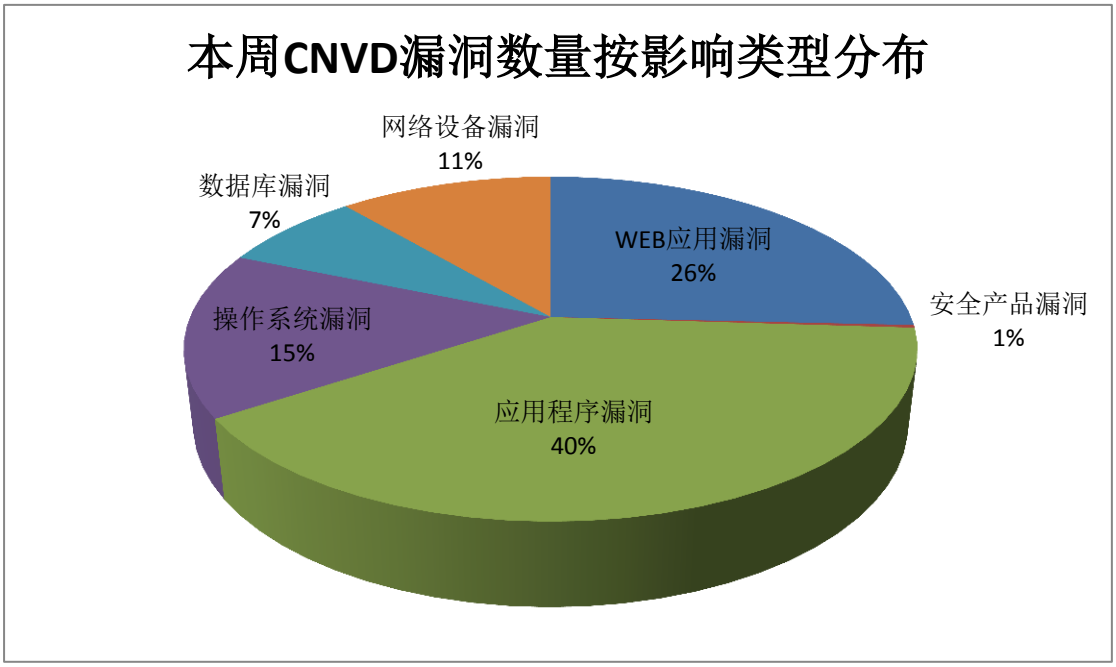

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Apple、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	Oracle	46	12%
2	Apple	35	9%
3	IBM	19	5%
4	Microsoft	16	4%
5	Cisco	15	3%
6	Rockwell Automation	12	3%
7	Google	10	2%
8	WordPress	10	2%
9	Frog CMS	6	2%
10	其他	231	58%

本周行业漏洞收录情况

本周，CNVD 收录了 22 个电信行业漏洞，47 个移动互联网行业漏洞，23 个工控行业漏洞（如下图所示）。其中，“Cisco IOS XE Software 输入验证漏洞、多款 Apple 产

品 Security 缓冲区溢出漏洞、Samsung 移动设备设计漏洞、Vecna VGo Robot OS 命令注入漏洞、Schneider Electric Triconex Tricon 未授权操作漏洞”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/

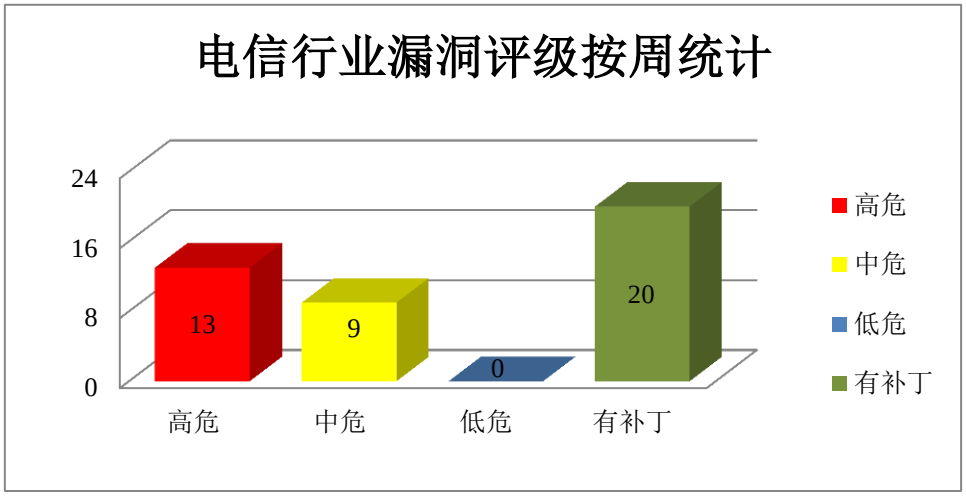

图 3 电信行业漏洞统计

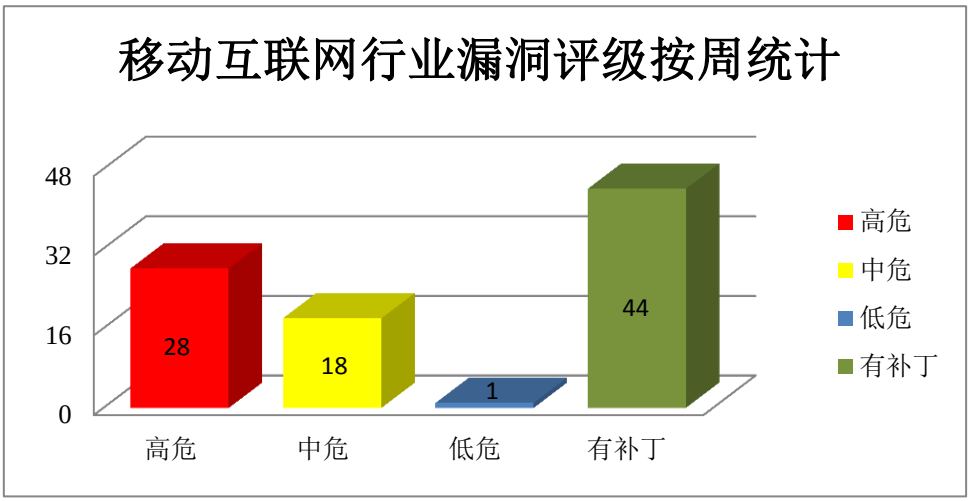

图 4 移动互联网行业漏洞统计

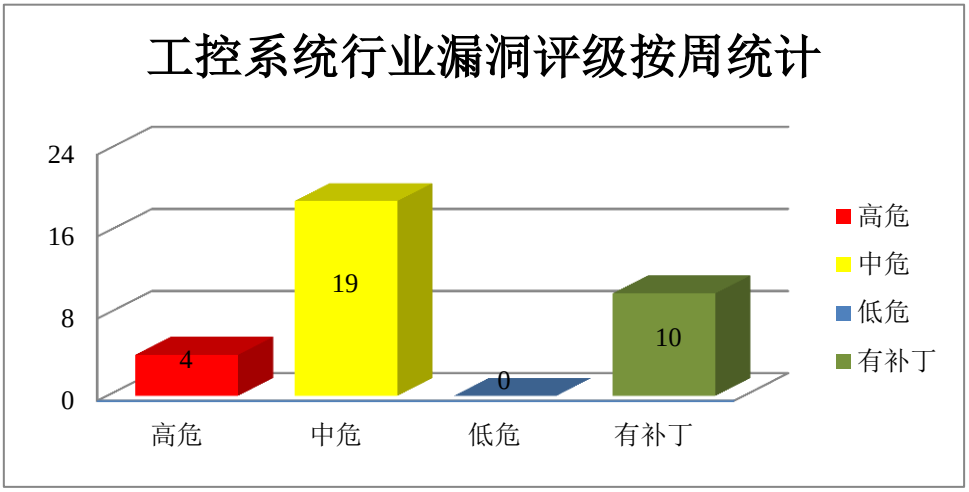

图 5 工控行业漏洞统计

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、Drupal Core 远程代码执行漏洞

Drupal 是一个由 Dries Buytaert 创立的自由开源的内容管理系统。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞远程执行代码。

CNVD 收录的相关漏洞包括：Drupal Core 远程代码执行漏洞。该漏洞的综合评级为“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-2018-08523

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。iCloud for Windows 是一款基于 Windows 平台的云服务。WebKit 是其中的一个 Web 浏览器引擎组件。本周，上述产品被披露存在内存破坏和缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：多款 Apple 产品 Kernel 内存破坏漏洞（CNVD-2018-08234、CNVD-2018-08235、CNVD-2018-08247、CNVD-2018-08249）、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-08242、CNVD-2018-08243、CNVD-2018-08266）、多款 Apple 产品 Security 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-2018-08234

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08235

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08247

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08249

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08242

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08243

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08266

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08298

3、Rockwell Automation 产品安全漏洞

Allen Bradley Micrologix 1400 Series B FRN 是美国罗克韦尔（Rockwell Automation）公司的一款可编程逻辑控制器。本周，上述产品被披露存在访问控制漏洞，攻击者可利用漏执行任意代码等。

CNVD 收录的相关漏洞包括：Allen Bradley Micrologix 1400 Series B FRN 访问控制漏洞（CNVD-2018-08279、CNVD-2018-08280、CNVD-2018-08281、CNVD-2018-08282、CNVD-2018-08283、CNVD-2018-08284、CNVD-2018-08285、CNVD-2018-08286）。上述漏洞的综合评级为“高危”。目前，厂商尚未发布漏洞修补程序。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-2018-08279

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08280

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08281

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08282

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08283

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08284

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08285

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08286

4、Microsoft 产品安全漏洞

Microsoft Excel 2010 SP2 是美国微软（Microsoft）公司 Office 套件中的一套电子表格处理软件。Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2008 SP2 是一套服务器操作系统。JET Database Engine 是其中的一个底层数据库引擎。本周，上述产品被披露存在远程代码执行和权限提升漏洞，攻击者可利用漏洞执行任意代码或提升权限。

CNVD 收录的相关漏洞包括：Microsoft Excel 远程代码执行漏洞（CNVD-2018-08416）、Microsoft Jet Database Engine 任意代码执行漏洞、Microsoft Windows kernel 本地权限提升漏洞（CNVD-2018-08190）、Microsoft Windows 远程代码执行漏洞（CNVD-2018-08336、CNVD-2018-08491、CNVD-2018-08492、CNVD-2018-08493、CNVD-2018-08494）。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-2018-08416

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08342

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08190

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08336

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08491

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08492

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08493

http://www.cnvd.org.cn/flaw/show/CNVD-2018-08494

5、Moxa AWK-3131A Wireless Access Point 硬编码管理员证书漏洞

Moxa AWK-3131A Wireless Access Point 是摩莎（Moxa）公司的一款无线交换机。本周，Moxa 被披露存在硬编码管理员证书漏洞，攻击者可利用该漏洞完全控制设备。目前，厂商尚未发布漏洞修补程序。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-2018-08325

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-2018-08096	PJSIP PJSUA2 SDK for Android 任意代码执行漏洞	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：http://www.pjsip.org/
CNVD-2018-08098	MetaIO SDK for Android 任意代码执行漏洞	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：http://www.metaio.com/sdk/
CNVD-2018-08099	Jumio SDK for Android 任意代码执行漏洞	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.jumio.com/
CNVD-2018-08448	Schneider Electric Triconex Tricon 未授权操作漏洞	高	用户可联系供应商获得补丁信息：https://ics-cert.us-cert.gov/advisories/ICSA-18-107-02
CNVD-2018-08450	Vecna VGo Robot OS 命令注入漏洞	高	用户可联系供应商获得补丁信息：https://ics-cert.us-cert.gov/advisories/ICSA-18-114-01
CNVD-2018-08469	Samsung 移动设备设计漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.samsungmobile.com/securityUpdate.smsb
CNVD-2018-08481	Etherpad 任意代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://blog.etherpad.org/2018/04/07/important-release-1-6-4/

CNVD-2018-08523	Drupal Core 远程代码执行漏洞	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-2018-004
CNVD-2018-08529	Atlassian Sourcetree for Windows 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jira.atlassian.com/browse/SRCTREEWIN-8509
CNVD-2018-08561	Kliqqi CMS SQL 注入漏洞	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.plikli.com/

小结：本周，Drupal 被披露存在远程代码执行漏洞，攻击者可利用漏洞远程执行代码。此外，Apple、Rockwell Automation、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限或发起拒绝服务攻击等。另外，Moxa 被披露存在硬编码管理员证书漏洞，攻击者可利用该漏洞完全控制设备。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。

本周漏洞要闻速递

1. 多品牌工业控制器存在拒绝服务（DoS）漏洞

4 月 28 日讯 工业网络安全公司 Applied Risk 的研究人员正在进行一项针对工业控制系统安全控制器的一项研究，他们分析了西门子、ABB、罗克韦尔、Allen Bradley、皮尔兹（Pilz）和菲尼克斯（Phoenix Contact）等几个大型厂商的安全控制器之后发现，这些控制器中可能存在严重的拒绝服务（DoS）漏洞 CVE-2017-9312。恶意攻击者可能会利用该漏洞发送发送以空操作（NOP）选项开始的 TCP 数据包，致使进入控制器拒绝服务状态。

参考链接：https://www.easyaq.com/news/1019255377.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