国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 10 月 22 日-2018 年 10 月 28 日 **2018 年第 43 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 79 个、中危漏洞 116 个、低危漏洞 5 个。漏洞平均分值为 6.13。本周收录的漏洞中，涉及 0day 漏洞 65 个（占 33%），其中互联网上出现“TP-Link TL-WR840N 和 TL-WR841N 认证绕过漏洞、D-link DSL-2640T 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 914 个，与上周（739 个）环比增长 24%。

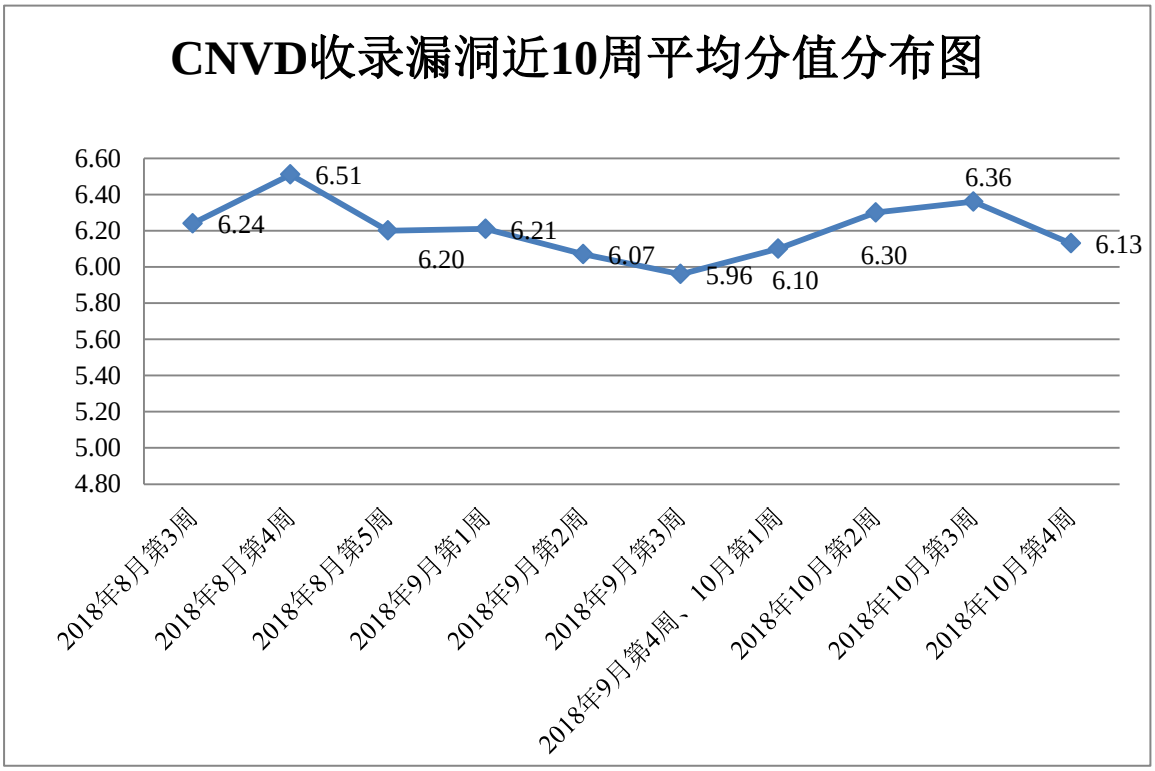

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 1 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 34 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 257 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 31 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 11 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：

上海斐讯数据通信技术有限公司、拓之林(北京)文化传播有限公司、锐捷网络股份有限公司、农夫山泉股份有限公司、掌易科技公司、上海维程计算机信息技术有限公司、长春凌展软件有限责任公司、上海寻梦信息技术有限公司、《中国科学》杂志社有限责任公司、安徽天达网络科技有限公司、长沙米拓信息技术有限公司、银川迅雷网络科技有限公司、南京南软科技有限公司、开普互联科技有限公司、淄博闪灵网络科技有限公司、深圳市荣光信息有限公司、中核建材有限公司、广州市巨硅信息科技有限公司、深圳市锟铻科技有限公司、北京费尔之盾科技有限公司、北京杰控科技有限公司、镇江市云优网络科技有限公司、北京新启科技有限公司、北京友华宇佳科技有限公司、北京广易东方信息技术有限公司、桂林崇胜网络科技有限公司、上海必智软件有限公司、普元信息技术股份有限公司、中国设备工程杂志网、国家公务员考试网、《中国质量万里行》杂志社、杨子晚报、老班 CMS、新秀工作室、飞飞影视导航系统（FeiFeiCms）、中文在线、春杰工作室、八哥软件、gxlcms、Duomicms、YCCMS。

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、新华三技术有限公司、北京神州绿盟科技有限公司、中国电信集团系统集成有限责任公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京圣博润高新技术股份有限公司、任子行网络技术股份有限公司、中新网络信息安全股份有限公司、北京明朝万达科技股份有限公司（安元实验室）、山石网科通信技术有限公司、北京智游网安科技有限公司、安徽锋刃信息科技有限公司、北京国舜科技股份有限公司、广州竞远安全技术股份有限公司、新疆海狼科技有限公司及其他个人白帽子向 CNVD 提交了 914 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 510 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

360 网神（补天平台）	270	270
漏洞盒子	240	240
北京天融信网络安全技术有限公司	197	22
哈尔滨安天科技股份有限公司	187	0
新华三技术有限公司	147	0
北京神州绿盟科技有限公司	147	0
中国电信集团系统集成有限责任公司	136	0
蓝盾信息安全技术有限公司	113	0
华为技术有限公司	93	0
恒安嘉新(北京)科技股份公司	37	0
北京数字观星科技有限公司	30	0
北京知道创宇信息技术有限公司	30	29
深圳市深信服电子科技有限公司	8	0
北京启明星辰信息安全技术有限公司	2	2
杭州安恒信息技术有限公司	1	1
山东云天安全技术有限公司	103	103
远江盛邦（北京）网络安全科技股份有限公司	32	32
北京圣博润高新技术股份有限公司	25	25
任子行网络技术股份有限公司	14	14
中新网络信息安全股份有限公司	7	7
北京明朝万达科技股份有限公司（安元实验室）	2	2
山石网科通信技术有限公司	1	1

北京智游网安科技有限公司	1	1
安徽锋刃信息科技有限公司	1	1
北京国舜科技股份有限公司	1	1
广州竞远安全技术股份有限公司	1	1
新疆海狼科技有限公司	1	1
CNCERT 贵州分中心	8	8
CNCERT 天津分中心	4	4
CNCERT 新疆分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 山西分中心	1	1
CNCERT 广东分中心	1	1
个人	143	143
报送总计	1988	914

本周漏洞按类型和厂商统计

本周，CNVD 收录了 200 个漏洞。应用程序漏洞 120 个，WEB 应用漏洞 34 个，数据库漏洞 20 个，网络设备漏洞 17 个，安全产品漏洞 7 个，操作系统漏洞 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
应用程序漏洞	120
WEB 应用漏洞	34
数据库漏洞	20
网络设备漏洞	17
安全产品漏洞	7
操作系统漏洞	2

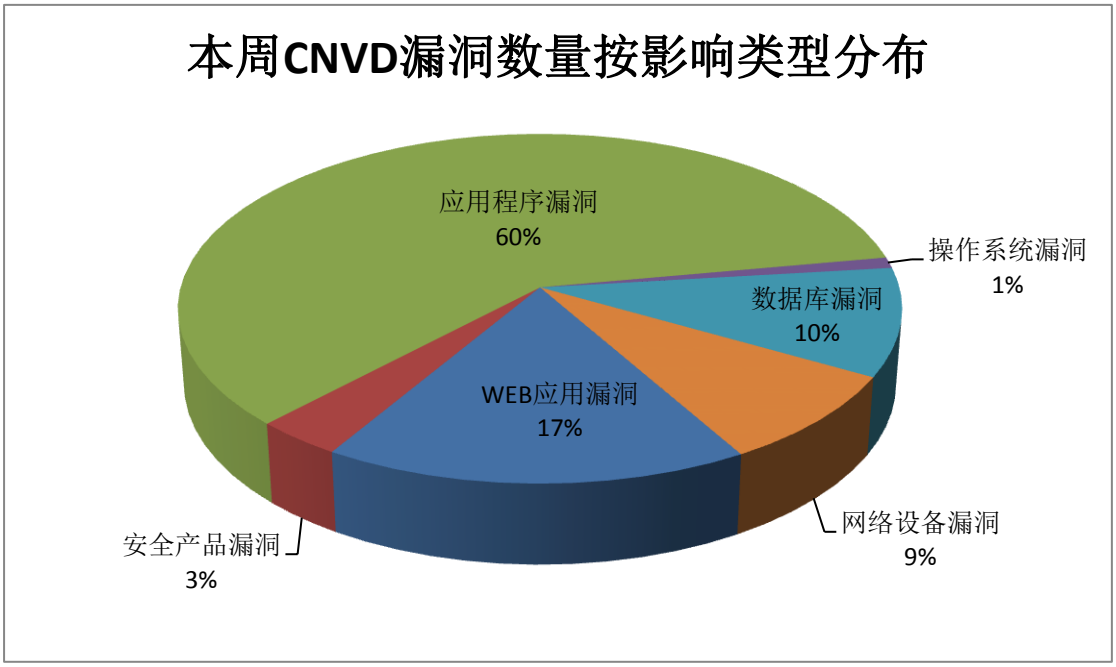

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Foxit、Mozilla 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	21	11%
2	Foxit	20	10%
3	Mozilla	16	8%
4	Cisco	14	7%
5	Advantech	8	4%
6	MOXA	8	4%
7	WordPress	6	3%
8	Destoon	4	2%
9	TP-LINK	4	2%
10	其他	99	49%

本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，4 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Advantech WebAccess 不当访问控制漏洞、Moxa EDR-810 命令注入漏洞、Cisco Webex Meetings Desktop App Update Service 命令注入漏洞、

Telecrane F25 Series 命令执行漏洞、Advantech WebAccess 任意文件删除漏洞”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/

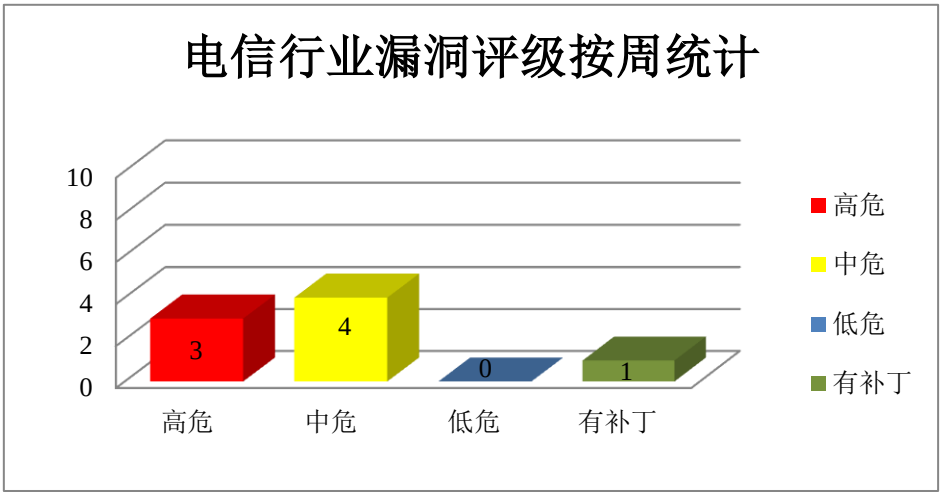

图 3 电信行业漏洞统计

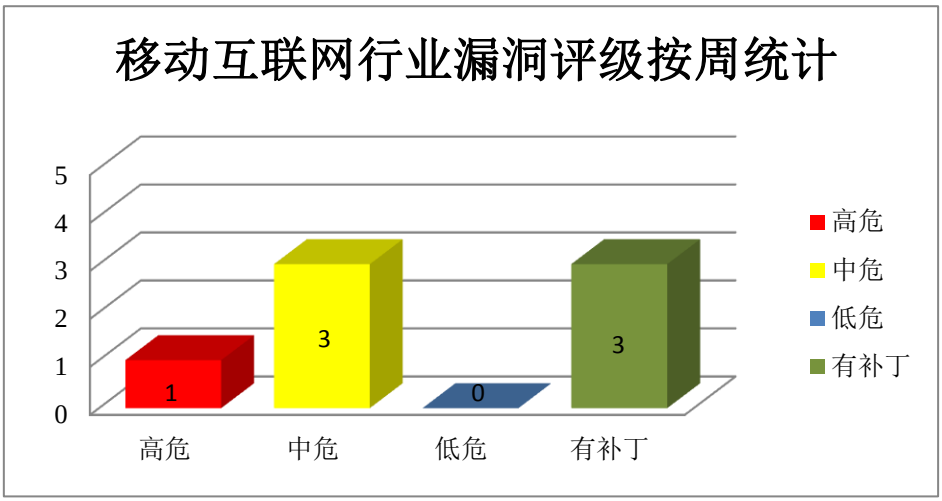

图 4 移动互联网行业漏洞统计

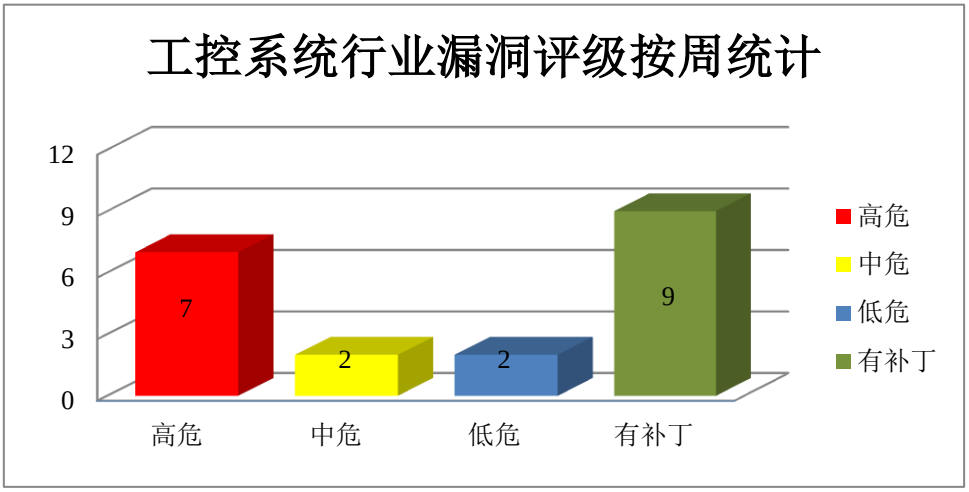

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle MySQL 是一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞造成拒绝服务（挂起或频繁崩溃），影响数据的可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2018-21471、CNVD-2018-21472、CNVD-2018-21474、CNVD-2018-21475、CNVD-2018-21478、CNVD-2018-21477、CNVD-2018-21486、CNVD-2018-21485）。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-2018-21471

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21472

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21474

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21475

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21478

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21477

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21486

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21485

2、Foxit 产品安全漏洞

Foxit Reader for Windows 是一款基于 Windows 平台的 PDF 文档阅读器。Foxit PhantomPDF for Windows 是它的商业版。本周，上述产品被披露存在内存错误引用漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 Foxit PhantomPDF for Windows 内存错误引用漏洞（CNVD-2018-21836、CNVD-2018-21837、CNVD-2018-21838、CNVD-2018-21839、CNVD-2018-21840、CNVD-2018-21841、CNVD-2018-21842、CNVD-2018-21843）。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-2018-21836
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21837
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21838
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21839
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21840
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21841
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21842
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21843

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器；Mozilla Firefox ESR 是 Firefox 的一个延长支持版本。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内存地址，执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2018-21814）、Mozilla Firefox 内存错误引用漏洞（CNVD-2018-21815、CNVD-2018-21816）、Mozilla Firefox 和 Firefox ESR 栈越界读取漏洞、Mozilla Firefox 内存破坏漏洞（CNVD-2018-21819）、Mozilla Firefox 代码执行漏洞（CNVD-2018-21820）、Mozilla Firefox 和 Firefox ESR 类型混淆漏洞、Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（CNVD-2018-21822）。其中，除“Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（CNVD-2018-21822）”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-2018-21814
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21815
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21816
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21817
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21819
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21820
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21821
http://www.cnvd.org.cn/flaw/show/CNVD-2018-21822

4、Cisco 产品安全漏洞

Cisco Wireless LAN Controller（WLC）Software 是一套用于配置和管理 WLC（无线

局域网控制器）的软件。Control and Provisioning of Wireless Access Points（CAPWAP）是其中的一个无线接入点控制和配置组件。Cisco WebEx Meetings 是网络会议解决方案。Cisco Firepower Threat Defense 是一套运行在防火墙中的软件。Cisco Digital Network Architecture Center（DNA Center）是一套数字网络体系结构解决方案。Cisco HyperFlex Software 是一套可扩展的分布式文件系统。Cisco Firepower System Software 是一款下一代防火墙产品（NGFW）。本周，该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，检索和修改重要的系统文件，运行任意命令，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2018-21481）、Cisco Webex Meetings Desktop App Update Service 命令注入漏洞、Cisco Firepower Threat Defense Software 拒绝服务漏洞、Cisco Digital Network Architecture Center 认证绕过漏洞、Cisco HyperFlex Static Signing Key 授权绕过漏洞、Cisco Firepower System Software Detection Engine 拒绝服务漏洞、Cisco Firepower System Software 命令执行漏洞、Cisco Digital Network Architecture Center 认证绕过漏洞。上述漏洞的综合评级为“高危”。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-2018-21481

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21739

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21924

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21926

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21928

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21929

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21930

http://www.cnvd.org.cn/flaw/show/CNVD-2018-21931

5、TP-Link TL-WA850RE Wi-Fi Range Extender 堆缓冲区溢出漏洞

TP-Link TL-WA850RE Wi-Fi Range Extender 是中国普联（TP-LINK）公司的一款无线网络信号扩展器。本周，TP-Link TL-WA850RE Wi-Fi Range Extender 被披露存在堆缓冲区溢出漏洞。远程攻击者可通过向 to/data/syslog.filter.json 文件发送较长的‘type’参数利用该漏洞造成拒绝服务（运行中断）。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-2018-21917

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-2018-21464	LIVE555 RTSP Server 缓冲区溢出漏洞	高	LIVE555 Streaming Media 已经发布补丁修复了上述漏洞，受影响的用户

			请尽快升级进行防护：http://www.live555.com/liveMedia/
CNVD-2018-21467	Zoho ManageEngine OpManager 任意文件上传漏洞	高	用户可联系供应商获得补丁信息：https://www.manageengine.com
CNVD-2018-21504	ThinkPHP SQL 注入漏洞（CNVD-2018-21504）	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/top-think/thinkphp/commit/77306720d5cbdf0fa97be9dea102a373a401f422
CNVD-2018-21511	Moxa ThingsPro 权限提升漏洞	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.moxa.com/
CNVD-2018-21606	Pydio 远程代码执行漏洞（CNVD-2018-21606）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://coastalsec.io/cve-2018-14772-remote-code-execution
CNVD-2018-21612	Info-ZIP UnZip 缓冲区溢出漏洞（CNVD-2018-21612）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugzilla.suse.com/show_bug.cgi?id=1110194
CNVD-2018-21735	Puppet Enterprise、razor-server 和 pe-razor-server 预安装漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://puppet.com/security/cve/CVE-2018-6512
CNVD-2018-21789	Pippo FastjsonEngine Fastjson 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/encyclopedia/ips/44059
CNVD-2018-21922	McAfee Threat Intelligence Exchange Server 代码注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kc.mcafee.com/corporate/index?page=content&id=SB10207
CNVD-2018-21920	Telecrane F25 Series 命令执行漏洞	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.telecrane.ca/

小结：本周，Oracle 被披露存在拒绝服务漏洞，攻击者可利用漏洞造成拒绝服务（挂起或频繁崩溃），影响数据的可用性。此外，Foxit、Mozilla、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取内存地址，绕过身份验证，执行任意代码，发起拒绝服务攻击等。另外，TP-Link TL-WA850RE Wi-Fi Range Extender 被披露存在堆缓冲区溢出漏洞。远程攻击者可通过向 to/data/syslog.filter.json 文件发送较长的‘type’参数利用该漏洞造成拒绝服务（运行中断）。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、D-link DSL-2640T 跨站脚本漏洞

验证描述

D-link DSL-2640T 是友讯（D-Link）公司的一款无线路由器。

D-link DSL-2640T 中的 cgi-bin/webcm 页面存在跨站脚本漏洞。远程攻击者可借助'var:RelaodHref'或'var:conid'参数利用该漏洞注入任意的 Web 脚本或 HTML。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2018100107

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-21854

信息提供者

恒安嘉新(北京)科技股份公司

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. UWP API 曝安全漏洞,可窃取任意数据

相关证据表明 Windows 10 系统中的 UWP API 存在严重安全漏洞，允许开发人员远程遍历你的磁盘信息，并窃取你的任意数据。UWP 应用由于使用沙盒机制，并且限定在自身路径和特殊文件夹内，因此具备较高的安全系数。

参考链接：https://www.cnbeta.com/articles/tech/781361.htm

2. X.Org 提权漏洞（CVE-2018-14665）

X.Org 存在严重的提权漏洞，漏洞产生于服务器对两个参数验证不正确，分别是"-modulepath 与-logfile"其中-modulepath 参数可用来指定一个不安全的路径，并跨权限执行代码，-logfile 参数则可用来在文件系统中实现任意文件覆盖。攻击者可利用这个漏洞特性实现提权（攻击者用户安装且可使用 X.Org）。

参考链接：https://www.anquanke.com/post/id/162843

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