国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 11 月 19 日-2018 年 11 月 25 日 **2018 年第 47 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 153 个，其中高危漏洞 61 个、中危漏洞 82 个、低危漏洞 10 个。漏洞平均分值为 6.27。本周收录的漏洞中，涉及 0day 漏洞 38 个（占 25%），其中互联网上出现“WordPress TemplateOne Themes Dubicars Database Backup 信息泄露漏洞、Budabot 拒绝服务漏洞”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 1352 个，与上周（1289 个）环比增长 5%。

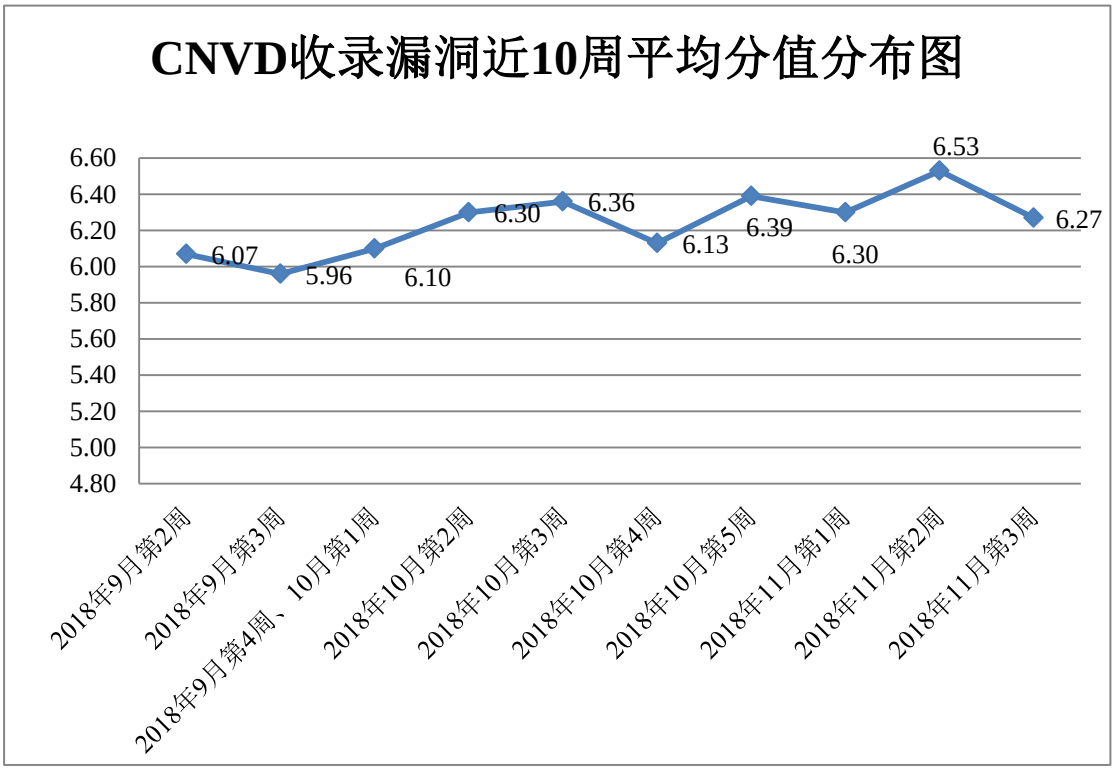

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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、证券、保险、能源等重要行业单位通报漏洞事件 27 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 179 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 66 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 20 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：

金山软件股份有限公司、杭州雄迈信息技术有限公司、长沙米拓信息技术有限公司、北京海腾时代科技有限公司、北京江民新科技术有限公司、深圳市图美电子技术有限公司、福州网钛软件科技有限公司、东莞市东域信息技术有限公司、南京同享网络科技有限公司、随州博强网络科技有限公司、深圳市中网互联网络科技开发有限公司、上海商创网络科技有限公司、大聪网络科技公司、杭州精英在线教育科技股份有限公司、上海智休信息科技有限公司、沧州市凡诺广告传媒有限公司、成都蜀美网络技术有限公司、金华市宁志网络科技有限公司、北京五指互联科技有限公司、青岛易软天创网络科技有限公司、中控太科（上海）电子科技有限公司、镇江市云优网络科技有限公司、联想集团、石家庄博士德软件科技开发有限公司、深圳市锟铻科技有限公司、济南华阳久泰信息技术有限公司、GNOME、微赞 CMS、Phpcms、老班 CMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技股份有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、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、北京信联科汇科技有限公司、中新网络信息安全股份有限公司、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、河南信安世纪科技有限公司、山石网科通信技术有限公司及其他个人白帽子向 CNVD 提交了 1352 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 910 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	501	501
360 网神（补天平台）	409	409

哈尔滨安天科技股份有限公司	181	0
华为技术有限公司	130	0
北京天融信网络安全技术有限公司	118	2
新华三技术有限公司	113	0
中国电信集团系统集成有限责任公司	82	0
北京神州绿盟科技有限公司	68	0
北京数字观星科技有限公司	68	0
深信服科技股份有限公司	25	0
恒安嘉新(北京)科技股份公司	6	0
杭州安恒信息技术有限公司	2	2
四川无声信息技术有限公司	1	1
山东云天安全技术有限公司	97	97
远江盛邦（北京）网络安全科技股份有限公司	18	18
北京圣博润高新技术股份有限公司	15	15
北京信联科汇科技有限公司	13	13
中新网络信息安全股份有限公司	13	13
安徽锋刃信息科技有限公司	5	5
北京国舜科技股份有限公司	2	2
广州竞远安全技术股份有限公司	2	2
河南信安世纪科技有限公司	2	2
山石网科通信技术有限公司	1	1
CNCERT 海南分中心	12	12

CNCERT 湖南分中心	7	7
CNCERT 天津分中心	4	4
CNCERT 吉林分中心	3	3
CNCERT 北京分中心	2	2
CNCERT 广东分中心	1	1
个人	240	240
报送总计	2141	1352

本周漏洞按类型和厂商统计

本周，CNVD 收录了 153 个漏洞。应用程序漏洞 119 个，网络设备漏洞 18 个，WEB 应用漏洞 11 个，操作系统漏洞 4 个，数据库漏洞 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	119
网络设备漏洞	18
WEB 应用漏洞	11
操作系统漏洞	4
数据库漏洞	1

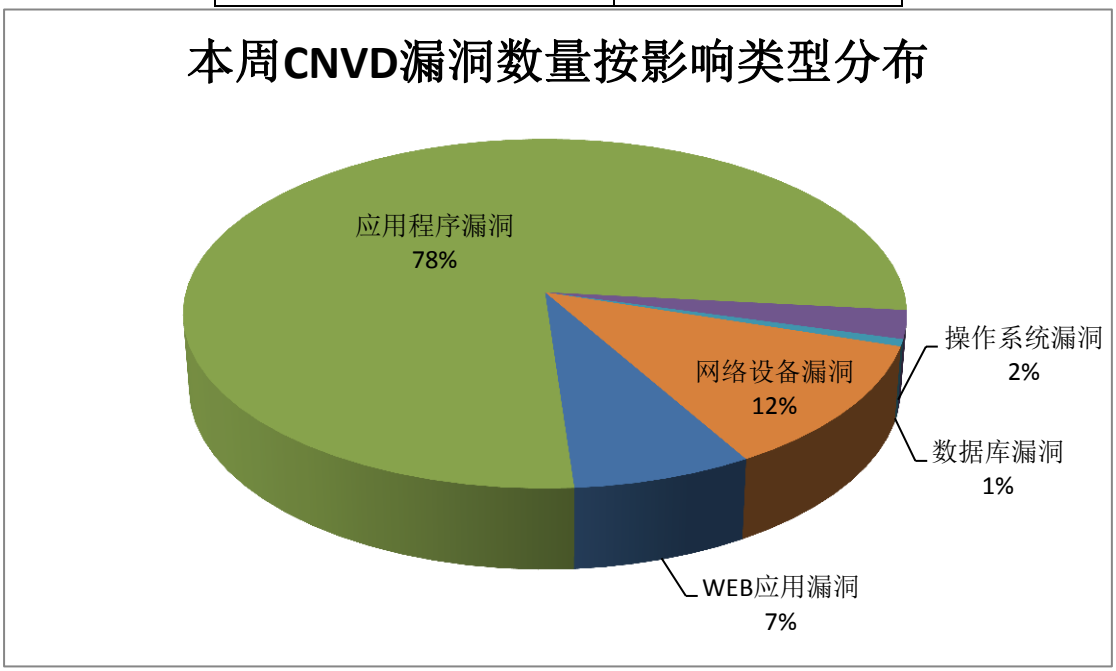

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Foxit、Google 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	18	12%
2	Foxit	11	7%
3	Google	8	5%
4	Microsoft	8	5%
5	Axis	6	4%
6	Dell	6	4%
7	perfSONAR	4	3%
8	TP-Link	4	3%
9	Cisco	3	2%
10	其他	85	55%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，11 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“Novell NetWare 栈缓冲区溢出漏洞、Cisco NX-OS 拒绝服务漏洞（CNVD-2018-23894）、TP-Link TL-R600VPN HTTP Server 缓冲区溢出漏洞、Open-Xchange OX App Suite readerengine 组件目录遍历漏洞、Siemens SIMATIC S7-400 输入验证漏洞”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/

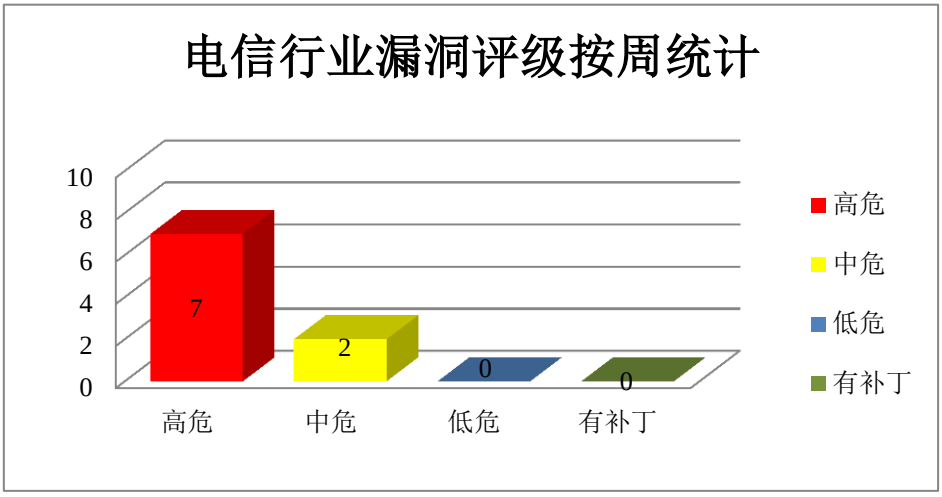

图 3 电信行业漏洞统计

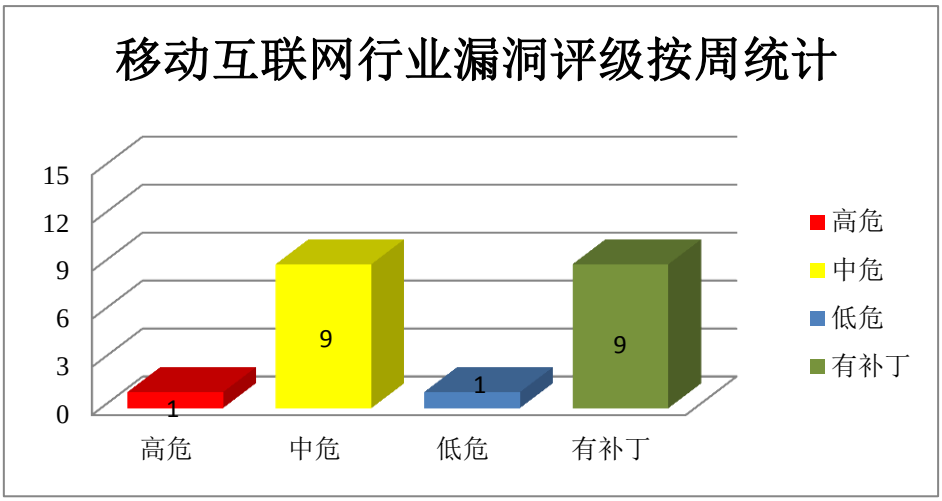

图 4 移动互联网行业漏洞统计

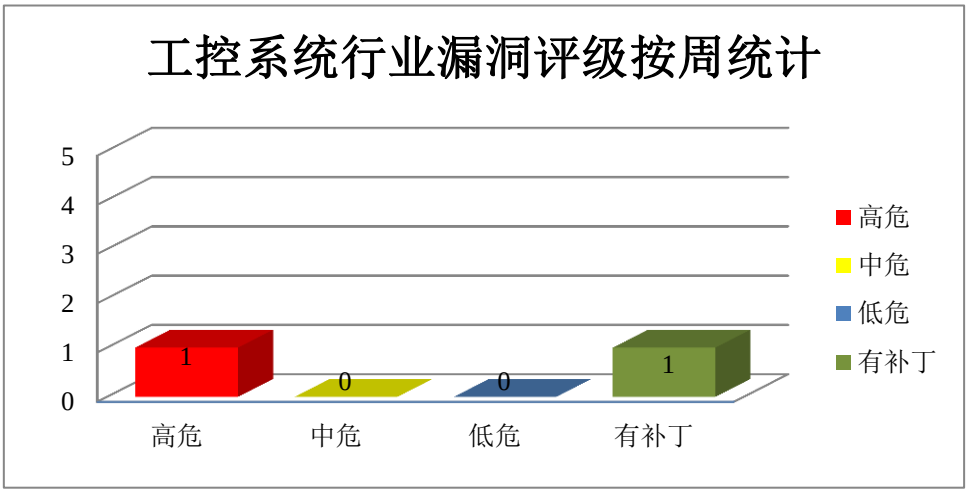

图 5 工控系统行业漏洞统计

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（又名 APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM WebSphere MQ 是一款消息传递中间件产品。IBM WebSphere Portal 是构建和管理 Web 门户的企业软件。其提供对 Web 内容和应用程序的访问，同时为用户提供个性化体验。IBM Rational Engineering Lifecycle Manager 可视化、分析及组织工程生命周期数据和数据关系。IBM Security Key Lifecycle Manager 使加密密钥管理流程集中化、简化和自动化，帮助最大限度降低加密密钥管理的风险和运营成本。IBM OpenPages GRC Platform 是一套用于管理企业风险和合规性的平台。IBM Cloud Private 是一套企业私有云解决方案。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，执行恶意的命令，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM API Connect CSV 注入漏洞、IBM WebSphere MQ 拒绝服务漏洞（CNVD-2018-23884）、IBM WebSphere Portal 开放重定向漏洞（CNVD-2018-23906）、IBM Rational Engineering Lifecycle Manager XML 外部实体注入漏洞、IBM Security Key Lifecycle Manager 认证缺失漏洞、IBM Security Key Lifecycle Manager 不当认证漏洞、IBM OpenPages GRC Platform 信息泄露漏洞（CNVD-2018-23915）、IBM Cloud Private 信息泄露漏洞。其中，除“IBM WebSphere MQ 拒绝服务漏洞（CNVD-2018-23884）、IBM OpenPages GRC Platform 信息泄露漏洞（CNVD-2018-23915）”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-2018-23883

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23884

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23906

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23908

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23911

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23912

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23915

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23916

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-2018-23724、CNVD-2018-23722、CNVD-2018-23723、CNVD-2018-23725、CNVD-2018-23726、CNVD-2018-23727、CNVD-2018-23729、CNVD-2018-23730）。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。C

NVD 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-2018-23724

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23722

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23723

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23725

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23726

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23727

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23729

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23730

3、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。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，提升权限，执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Google Android wcd_cpe_core 内存错误引用漏洞、Google Android MDSS 驱动程序拒绝服务漏洞、Google Android Kernel 拒绝服务漏洞、Google Chrome GPU 拒绝服务漏洞、Google gVisor 权限提升漏洞、Google Monorail 跨站点搜索漏洞（CNVD-2018-23925、CNVD-2018-23926、CNVD-2018-23927）。其中，“IBM Rational Quality Manager 权限提升漏洞”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-2018-23866

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23874

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23875

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23910

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23920

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23925

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23926

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23927

4、Microsoft 产品安全漏洞

Microsoft Excel 是一款电子表格处理软件。Microsoft Team Foundation Server 是一套应用程序生命周期管理（ALM）工具套件中的源代码管理、项目管理和团队协作平台。Microsoft Outlook 是一款 Office 套件中所捆绑的电子邮件客户端软件。Microsoft Word 是一款文字处理软件。Microsoft Windows 7 SP1 是一套个人电脑使用的操作系统。Windows Server 2008 R2 SP1 是一套服务器操作系统。Internet Explorer（IE）是其中的一

款 Windows 系统附带的浏览器。Bing Places for Business 是一个 Bing 门户网站，让本地企业主在 Bing 上为他们的业务添加一个列表。本周，该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，破坏内存等。

CNVD 收录的相关漏洞包括：Microsoft BingPlaces - TrackEmailOpen (url)开放重定向漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2018-23749）、Microsoft Team Foundation Server 跨站脚本漏洞、Microsoft Word 远程代码执行漏洞（CNVD-2018-23753）、Microsoft Outlook 信息泄露漏洞（CNVD-2018-23750、CNVD-2018-23751）、Microsoft Internet Explorer 信息泄露漏洞（CNVD-2018-23919）、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2018-23924）。其中，“Microsoft Excel 远程代码执行漏洞（CNVD-2018-23749）、Microsoft Word 远程代码执行漏洞（CNVD-2018-23753）、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2018-23924）”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-2018-23623

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23749

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23752

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23753

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23750

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23751

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23919

http://www.cnvd.org.cn/flaw/show/CNVD-2018-23924

5、Dell EMC ESRS Policy Manager 远程代码执行漏洞

Dell EMC ESRS 是戴尔公司一款安全远程支持服务程序，Policy Manager 可以为客户端管理的设备设置权限。本周，Dell EMC ESRS Policy Manager 被披露存在远程代码执行漏洞。攻击者可利用该漏洞在受影响应用程序中执行任意代码，失败的攻击会造成拒绝服务。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-2018-23922

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-2018-23613	RichFaces 表达式语言注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14667
CNVD-2018-23616	Intel Rapid Store Technology 输入验证漏洞	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.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00153.html
CNVD-2018-23622	Adobe Flash Player 任意代码执行漏洞（CNVD-2018-23622）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://helpx.adobe.com/security/products/flash-player/apsb18-44.html
CNVD-2018-23629	TP-Link TL-R600VPN HTTP Server 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.tp-link.com/us/products/details/cat-4909_TL-R600VPN.html
CNVD-2018-23755	Micro Focus Solutions Business Manager 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：http://help.serena.com/doc_center/sbm/ver11_4/sbm_release_notes.htm
CNVD-2018-23871	Axis IP Cameras 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf
CNVD-2018-23877	Open-Xchange OX App Suite readerengine 组件目录遍历漏洞	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.open-xchange.com/
CNVD-2018-23882	Novell NetWare 栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://download.novell.com/Download?buildid=1z3z-OsVCiE~
CNVD-2018-23893	Siemens SIMATIC S7-400 输入验证漏洞	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.industry.siemens.com/cs/ww/en/view/109476571
CNVD-2018-23896	Cisco FXOS 和 NX-OS 拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181017-fxnx-os-dos

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，执行恶意的命令，发起拒绝服务攻击等。此外，Foxit、Google、Microsoft 等多款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，提升权限，执行任意代码，破坏内存或发起拒绝服务攻击等。另外，Dell EMC ESRS Policy Manager 被披露存在远程代码执行漏洞。攻击者可利用该漏洞在受影响应用程序中执行任意代码，失败的攻击会造成拒绝服务。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、WordPress TemplateOne Themes Dubicars Database Backup 信息泄露漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress TemplateOne Themes Dubicars Database Backup 存在信息泄露漏洞。攻击者可利用漏洞获敏感信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=31482

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-23625

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. 大量 Android 第三方 ROM 未正确配置导致信息泄漏预警

近日，Magisk 作者 topjohnwu 发表文章，提到他在研究 Fate/Grand Order 手游的 root 检测机制时发现了存在于数百万台 android 设备上的漏洞，利用该漏洞会泄漏系统上的进程信息。

参考链接：https://www.anquanke.com/post/id/166475

2. Adobe Flash Player 任意代码执行漏洞（CVE-2018-15981）

最近，Adobe 发布适用于 Windows，macOS，Linux 和 Chrome OS 的 Adobe Flash Player 安全更新，修补了一枚类型混淆漏洞（CVE-2018-15981）。该漏洞影响 Adobe Flash Player 31.0.0.148 及以前版本，成功利用会导致任意代码执行。

参考链接：https://www.anquanke.com/post/id/164969

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