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 8 日-2018 年 10 月 14 日　　2018 年第 41 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 240 个，其中高危漏洞 85 个、中危漏洞 143 个、低危漏洞 12 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 48 个（占 20%），其中互联网上出现“D-Link DSL-2750B OS 命令注入漏洞、WordPress 插件 Pie Register 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 679 个，与上周（1261 个）环比下降 46%。

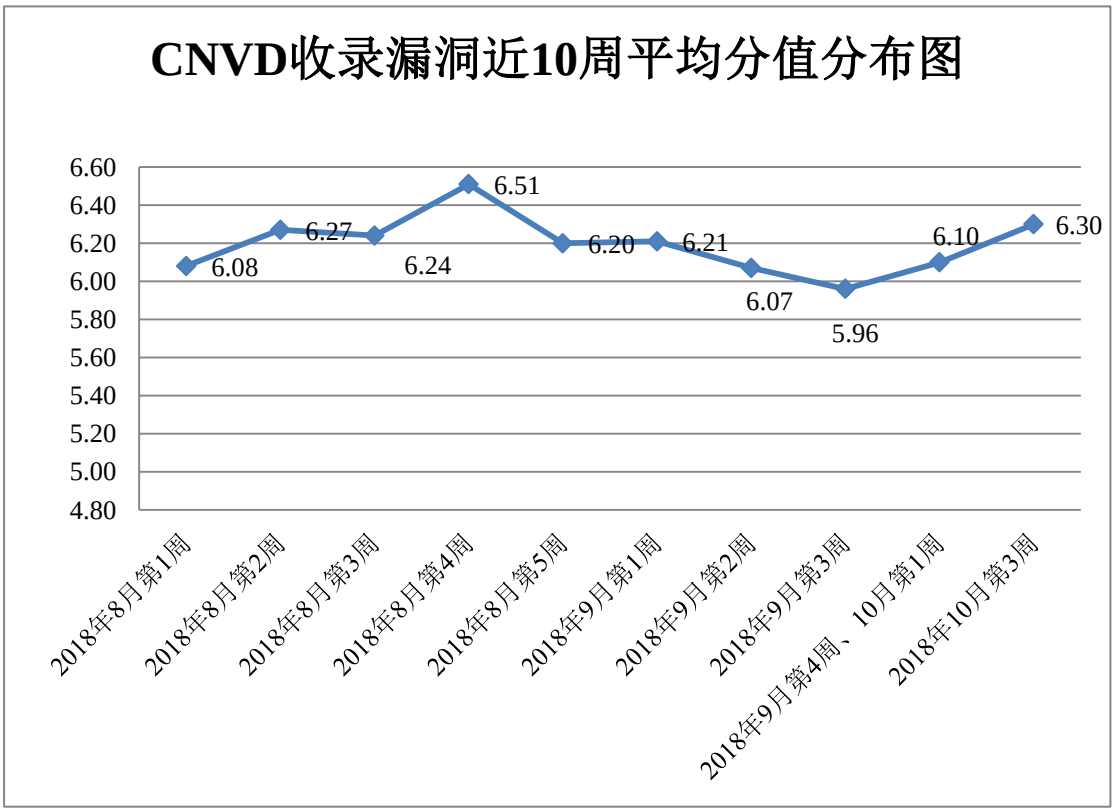

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 16 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 263 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 108 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 37 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：

中铁电气化铁路运营管理有限公司、镇江市云优网络科技有限公司、长沙翱云网络科技有限公司、宿迁鑫潮信息技术限公司、北京五指互联科技有限公司、珠海市魅族科技有限公司、搜狗公司、北京费尔之盾科技有限公司、锐捷网络股份有限公司、大唐云南发电有限公司、宁波市鄞州区天发网络科技有限公司、宁波天航国际物流有限公司、友讯电子设备（上海）有限公司、航天数字传媒有限公司、湖南梦行科技有限公司、中国水务集团有限公司、鼎点视讯科技有限公司、智士软件(北京)有限公司、南昌维网数字传媒有限公司、上海鸿庭信息科技有限公司、合肥谨宸网络科技有限公司、北京中税网控股股份有限公司、深圳市星垂科技有限公司、乐外资源分享网、财新网、中国软件和信息服务业务网、中国城乡新闻网、中国农机工业网、环球物流网、中国实事新闻社、中国汽车工业协会、速通物流、雷风影视、机械制造系统国家重点实验室、凌夕网络、石家庄市飞翔航空科技研究所、易迅软件、中国青少年军事夏令营、中国科协生命科学学会联合体、YCCMS、SemCms、phpdisk、iCMSdev。

本周，CNVD 发布了《Microsoft 发布 2018 年 10 月安全更新》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4707

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、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、北京启明星辰信息安全技术有限公司、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、北京圣博润高新技术股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、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、山石网科通信技术有限公司、河南信安世纪科技有限公司、广州竞远安全技术股份有限公司、新疆海狼科技有限公司、北京国舜科技股份有限公司、南京联成科技发展股份有限公司、北京明朝万达科技股份有限公司（安元实验室）及其他个人白帽子向 CNVD 提交了 67

9 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 350 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
新华三技术有限公司	332	0
北京天融信网络安全技术有限公司	279	3
哈尔滨安天科技股份有限公司	223	0
漏洞盒子	203	203
360 网神（补天平台）	147	147
北京启明星辰信息安全技术有限公司	134	1
中国电信集团系统集成有限责任公司	104	0
北京神州绿盟科技有限公司	103	0
华为技术有限公司	100	0
深圳市深信服电子科技有限公司	87	0
北京数字观星科技有限公司	69	0
恒安嘉新(北京)科技股份公司	50	0
北京知道创宇信息技术有限公司	44	37
山东云天安全技术有限公司	87	87
北京圣博润高新技术股份有限公司	26	26
远江盛邦（北京）网络安全科技股份有限公司	24	24
任子行网络技术股份有限公司	21	21
中新网络信息安全股份有限公司	19	19
山石网科通信技术有限公司	8	8

河南信安世纪科技有限公司	8	8
广州竞远安全技术股份有限公司	4	4
新疆海狼科技有限公司	4	4
北京国舜科技股份有限公司	3	3
南京联成科技发展股份有限公司	3	3
北京明朝万达科技股份有限公司（安元实验室）	2	2
CNCERT 湖南分中心	7	7
CNCERT 新疆分中心	4	4
CNCERT 北京分中心	2	2
CNCERT 贵州分中心	1	1
CNCERT 吉林分中心	1	1
个人	64	64
报送总计	2163	679

本周漏洞按类型和厂商统计

本周，CNVD 收录了 240 个漏洞。应用程序漏洞 158 个，网络设备漏洞 34 个，WEB 应用漏洞 24 个，操作系统漏洞 20 个，安全产品漏洞 3 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	158
WEB 应用漏洞	34
网络设备漏洞	24
操作系统漏洞	20
安全产品漏洞	3
数据库漏洞	1

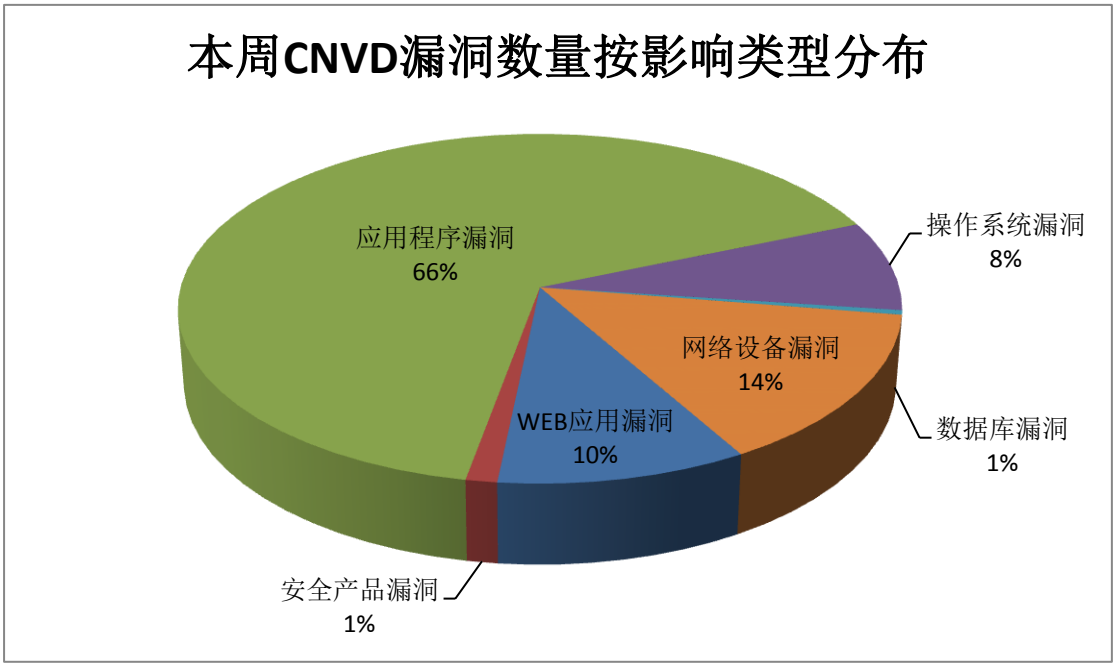

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Foxit、IBM、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	Foxit	39	16%
2	IBM	23	10%
3	Cisco	19	8%
4	Microsoft	11	5%
5	Google	10	4%
6	Apache	9	3%
7	AirTies	7	3%
8	D-Link	7	3%
9	Fuji Electric	4	2%
10	其他	111	46%

本周行业漏洞收录情况

本周，CNVD 收录了 15 个电信行业漏洞，12 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“Cisco 807、809 和 829 Industrial Integrated Services Router 任意内存写入漏洞、Google Android 'ihevcd_parse_sei_payload'函数远程代码执行漏洞、

Fuji Electric V-Server 缓冲区溢出漏洞、Symantec Norton App Lock 权限获取漏洞、SIEMENS SIMATIC S7-1200 CPU Family 跨站请求伪造漏洞”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/

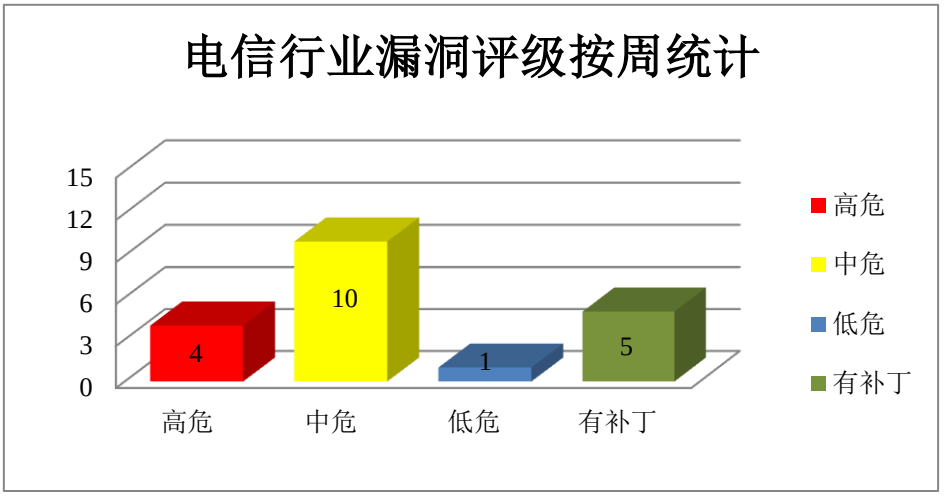

图 3 电信行业漏洞统计

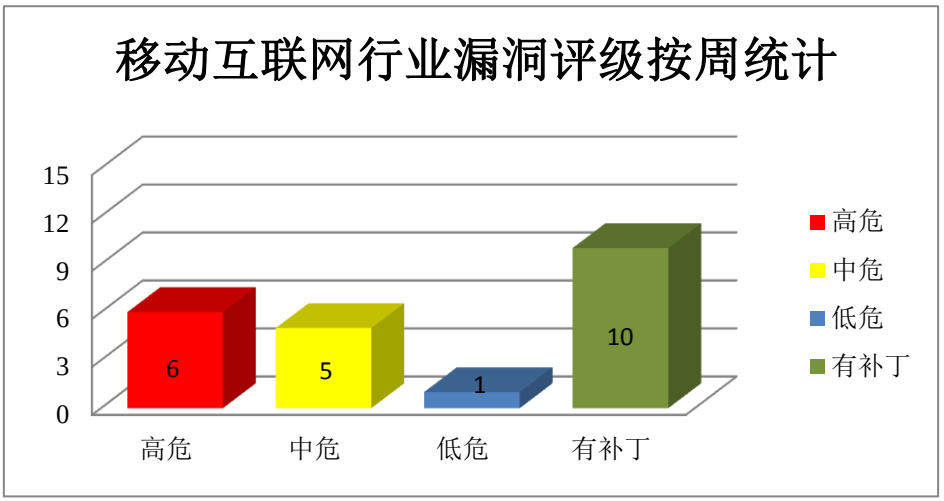

图 4 移动互联网行业漏洞统计

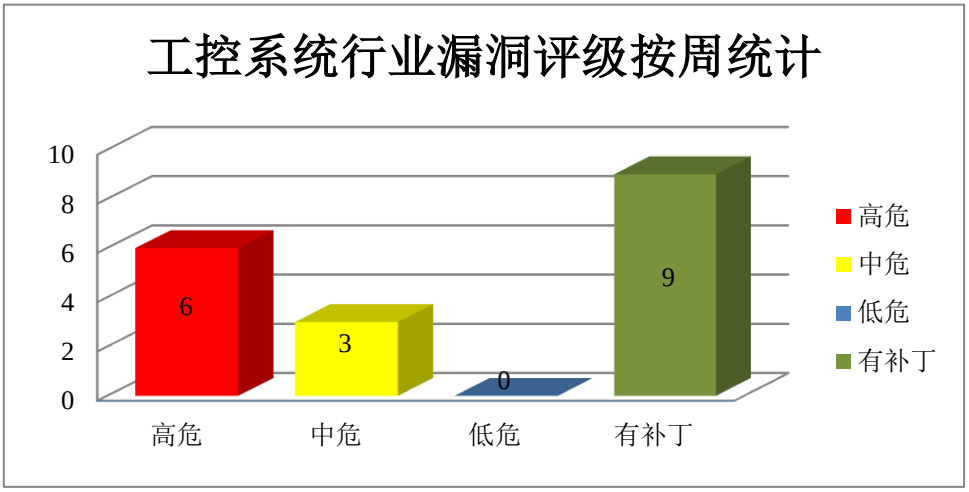

图 5 工控系统行业漏洞统计

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、Foxit 产品安全漏洞

Foxit PDF Reader 是一款 PDF 文档阅读器。JavaScript engine 是其中的一个 JavaScript 脚本引擎。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader JavaScript 引擎远程代码执行漏洞（CNVD-2018-20706、CNVD-2018-20707、CNVD-2018-20708、CNVD-2018-20709、CNVD-2018-20710、CNVD-2018-20711、CNVD-2018-20712、CNVD-2018-20713）。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-2018-20706

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20707

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20708

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20709

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20710

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20711

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20712

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20713

2、Microsoft 产品安全漏洞

Microsoft Windows Server 2008 SP2 是一套服务器使用的操作系统。Windows 10 是一套个人电脑使用的操作系统。PowerPoint Viewer 2007 是一款演示文稿处理程序。Microsoft Excel Viewer 2007 SP3 是一款电子表格处理程序。Internet Explorer 是一款

网页浏览器。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，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft Windows Graphics 组件信息泄露漏洞（CNVD-2018-20734）、Microsoft Windows Media Player 信息泄露漏洞、Microsoft Windows Graphics 组件远程执行代码漏洞（CNVD-2018-20739）、Microsoft Windows Theme API 远程执行代码漏洞、Microsoft Windows MS XML 远程执行代码漏洞、Microsoft Windows TCP/IP 信息泄露漏洞、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2018-20743、CNVD-2018-20736）。其中，除“Microsoft Windows Graphics 组件信息泄露漏洞（CNVD-2018-20734）、Microsoft Windows Media Player 信息泄露漏洞、Microsoft Windows TCP/IP 信息泄露漏洞”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-2018-20734
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20735
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20739
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20737
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20740
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20741
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20743
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20736

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，攻击者可利用漏洞执行任意代码（整数溢出和越界写入）等。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 组件权限提升漏洞（CNVD-2018-20744）、Google Chrome 地址栏欺骗漏洞（CNVD-2018-20745）、Google Android 'CollectValuesOrEntriesImpl'函数远程代码执行漏洞、Google Android 'copy_process'函数权限提升漏洞、Google Android 'ihevcd_parse_sei_payload'函数远程代码执行漏洞、Google Chrome WebAudio 越界读取漏洞、Google Chrome Skia 整数溢出漏洞（CNVD-2018-20752）、Google Chrome WebRTC 内存错误引用漏洞（CNVD-2018-20753）。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-2018-20744
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20745

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20746

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20747

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20748

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20749

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20752

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20753

4、Apache 产品安全漏洞

Apache Tomcat 是一款轻量级 Web 应用服务器。Apache Ranger 提供一个集中式安全管理框架，并解决授权和审计。Apache PDFBox 是一个开源的、基于 Java 并提供创建新的 PDF 文档、修改现有的 PDF 文档等功能的工具库。 Apache Tika 是一个集成了 POI（使用 Java 程序对 Microsoft Office 格式文档提供读和写功能的开源函数库）、Pdfbox（读取和创建 PDF 文档的纯 Java 类库）并为文本抽取工作提供了统一界面的内容抽取工具集合。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，覆盖文件，执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache Tomcat 开放重定向漏洞、Apache PDFBox parser 拒绝服务漏洞、Apache Tika 拒绝服务漏洞（CNVD-2018-20684）、Apache Tika XML 外部实体拒绝服务漏洞、Apache Tika 任意文件覆盖漏洞、Apache Mesos 信息泄露漏洞、Apache Tika 拒绝服务漏洞、Apache Ranger UnixAuthenticationService 缓冲区溢出漏洞。其中，“Apache Ranger UnixAuthenticationService 缓冲区溢出漏洞”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-2018-20302

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20305

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20684

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20788

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20789

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20787

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20790

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20791

5、ADB Epicentro 缓冲区溢出漏洞

ADB Epicentro 是一套使用在 ADB 网关和路由器设备中的固件。本周，ADB Epicentro 被披露存在缓冲区溢出漏洞。远程攻击者可借助特制的 GET 请求利用该漏洞造成拒绝服务。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-2018-20660

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-2018-20303	VMware Workspace ONE Unified Endpoint Management Console (AirWatch Console) SAML 身份验证绕过漏洞	高	用户可联系供应商获得补丁信息：https://www.vmware.com/security/advisories/VMSA-2018-0024.html
CNVD-2018-20399	Ektron Content Management System (CMS)远程重新启用用户漏洞	高	用户可联系供应商获得补丁信息：https://www.episerver.com
CNVD-2018-20531	SIEMENS SIMATIC S7-1200 CPU Family 跨站请求伪造漏洞	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://cert-portal.siemens.com/productcert/pdf/ssa-507847.pdf
CNVD-2018-20535	GhostScript 沙箱绕过漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：http://git.ghostscript.com/?p=ghostpdl.git;a=commitdiff;h=a6807394bd94
CNVD-2018-20574	Symantec Norton App Lock 权限获取漏洞	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.symantec.com/en_US/article.SYMSA1455.html
CNVD-2018-20656	QEMU 缓冲区溢出漏洞（CNVD-2018-20656）	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.qemu.org/
CNVD-2018-20661	REDAXO SQL 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://github.com/redaxo/redaxo/releases/tag/5.6.4
CNVD-2018-20678	Emerson AMS Device Manager 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://ics-cert.us-cert.gov/advisories/ICSA-18-270-01
CNVD-2018-20765	HPE Intelligent Management Center 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03893en_us
CNVD-2018-20767	Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2018-20767）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb18-30.html

小结：本周，Foxit 被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代

码。此外，Microsoft、Google、Apache 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，覆盖文件，执行任意代码，执行任意代码，破坏内存，发起拒绝服务攻击等。另外，ADB Epicentro 被披露存在缓冲区溢出漏洞。远程攻击者可借助特制的 GET 请求利用该漏洞造成拒绝服务。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、D-Link DSL-2750B OS 命令注入漏洞

验证描述

D-Link DSL-2750B 是一款 ADSL 路由器。

D-Link DSL-2750B 存在 OS 命令注入漏洞。攻击者可利用漏洞执行任意命令。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2018050223

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-20853

信息提供者

杭州安恒信息技术有限公司

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. 900 万台杭州雄迈科技生产的视频监控设备被曝 DVR 漏洞

安全研究人员发现杭州雄迈科技生产的视频监控设备存在安全漏洞，包括默认管理员密码（即无密码，初始设置没有强制设置密码）、“默认”帐户的不安全凭据、多个未加密信道、薄弱的更新机制和未签名的固件等。研究人员表示帮助用户连接到公司“XMEye P2P Cloud”并与设备进行交互操作的 ID 很容易通过设备的 MAC 地址获得，而且与云服务器提供商建立的链路（默认情况下已启用）没有加密，这些服务器的地理位置等信息暂时没有想请提供。最关键的是，设备的 P2P 云功能可以绕过防火墙并允许远程连接到专用网络，这也是之前成为 Mirai 僵尸网络重灾区的原因之一。

参考链接：https://www.helpnetsecurity.com/2018/10/10/vulnerable-xiongmai-cameras/

2. 加密聊天工具 Telegram 并不安全，用户通话会曝光 IP 地址

据外媒报道，Telegram 是一款可以让用户在互联网上与其他用户展开加密聊天和通话的通信应用。这款程序自称是一款安全的私人通信应用程序，然而一项研究发现，在

它的默认配置下，它会在用户通话过程中泄露出 IP 地址。在默认设置下，Telegram 的语音通话通过 P2P2 进行。当使用 P2P 的时候，用户通话对象的 IP 地址则会出现在 Telegram 控制日志上。不过不是所有的版本都有控制日志。比如 Windows 版不会，但 Linux 版却有。

参考链接：https://www.easyaq.com/news/637273528.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